EXHIBIT 9

Sent: 2/23/2020 1:48:18 PM
To: Randy Mead [rmead@ligtel.net]
Subject: 3GPP HNI guidelines
Attachments: 23003-g00.docx; 23012-f00.doc

Per our call with Shelley this morning I've compiled some information from 3GPP on HNI implementation guidelines for mobile networks. 3GPP is the international governing body responsible for mobile network standards. BaiCells claims to be 3GPP compliant in their documentation and on their website.

https://na.baicells.com/lte-network/

The IMSI is composed of the PLMN (MCC and MNC) as the first six digits (in the United States) and an additional nine digits for the MSIN (Mobile Subscriber Identification Number). I have attached documentation from 3GPP that defines the IMSI and how it is used on identifying carriers and routing traffic between them. It also defines how carriers are to be identified via the IMSI (Section 2.3). Here is the web link where I pulled the documentation:

https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=729

I've attached version 16.0.0 of the specification dated 9-18-2019.

3GPP Specification 23.012 defines how roaming authentication is supposed to take place between home and visitor networks. Primary information is in section 2 and 3. I've attached version 15.0.0 of the specification dated 6-22-2018.

Here is a basic walk through of how the IMSI is used when a device connects to a roaming network:

When an LTE device is switched on or transferred via handover to a network other than the home, the "visited" network sees the device due to the client responding to it's broadcasted carrier. The visited network notices that it is not registered with it's own system and attempts to identify the client's home network. It does this by looking at the client's IMSI. It looks up the carrier MCC/MNC to see if there is a roaming agreement. If there is no agreement service is denied by the visited network.

If there is a roaming agreement the visited network contacts the home network and requests service level information about the roaming device using the IMSI. If the lookup is successful the visited network begins to maintain a temporary subscriber record for the device. The home network will also update records to show that the roaming device is on the visited network so traffic can be directed appropriately.

Here is a link to technical blog that walks through the procedure:

https://www.netmanias.com/en/post/blog/5929/lte/lte-user-identifiers-imsi-and-guti

I'm hoping that this information will be helpful in explaining the importance of what the HNI means to a mobile network as a whole and how it allows interaction with other mobile networks.

Joshua Wentworth
Network Operations Supervisor
Ligtel Communications/Ligonier Telephone
260-894-7161

3GPP TS 23.003 V16.0.0 (2019-09)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Numbering, addressing and identification (Release 16)

Keywords
GSM, UMTS, addressing

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Specification (TS) has been produced by the 3rd Generation Partnership Project (3GPP).

The present document defines the principal purpose and use of International Mobile station Equipment Identities (IMEI) within the digital cellular telecommunications system and the 3GPP system.

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document defines the principal purpose and use of different naming, numbering, addressing and identification resources (i.e. Identifiers (ID)) within the digital cellular telecommunications system and the 3GPP system.

IDs that are covered by this specification includes both public IDs, private IDs and IDs that are assigned to MSs/UEs. Many of the IDs are used temporary in the networks and are allocated and assigned by the operators and some other IDs are allocated and assigned on either global, regional and national level by an administrator. See ITU-T Recommendation E.101 [122].

NOTE: Allocation means the process of opening a numbering, naming or addressing resource in a plan for the purpose of its use by a telecommunication service under specified conditions. The allocation in itself does not yet give rights for any user, whether an operator, service provider, user or someone else, to use the resource. Assignment means authorization given to an applicant for the right of use of number, naming or addressing resources under specified conditions.

The present document defines:

0) the principal purpose and use of International Mobile station Equipment Identities (IMEI) within the digital cellular telecommunications system and the 3GPP system

a) an identification plan for public networks and subscriptions in the 3GPP systems;

b) principles of assigning telephone numbers to MSs in the country of registration of the MS;

c) principles of assigning Mobile Station (MS) roaming numbers to visiting MSs;

d) an identification plan for location areas, routing areas, and base stations in the GSM system;

e) an identification plan for MSCs, SGSNs, GGSNs, and location registers in the GSM/UMTS system;

f) principles of assigning international mobile equipment identities;

g) principles of assigning zones for regional subscription;

h) an identification plan for groups of subscribers to the Voice Group Call Service (VGCS) and to the Voice Broadcast Service (VBS); and identification plan for voice group calls and voice broadcast calls; an identification plan for group call areas;

i) principles for assigning Packet Data Protocol (PDP) addresses to mobile stations;

j) an identification plan for point-to-multipoint data transmission groups;

k) an identification plan for CN domain, RNC and service area in the UTRAN system.

l) an identification plan for mobile subscribers in the WLAN system.

m) addressing and identification for IMS Service Continuity

n) an identification plan together with principles of assignment and mapping of identities for the Evolved Packet System; and

o) addressing and identification for Proximity-based (ProSe) Services.

p) an identification for Online Charging System (OCS).

q) an identification plan together with principles of assignment and mapping of identities for the 5G System.

The present document specifies functions, procedures and information which apply to GERAN Iu mode. However, functionality related to GERAN Iu mode is neither maintained nor enhanced.

1.1 References

1.1.1 Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 21.905: "Vocabulary for 3GPP Specifications ".

[2] 3GPP TS 23.008: "Organization of subscriber data".

[3] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2"

[4] 3GPP TS 23.070: "Routeing of calls to/from Public Data Networks (PDN)".

[5] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[6] 3GPP TS 29.060: "GPRS Tunnelling protocol (GTP) across the Gn and Gp interface".

[7] 3GPP TS 43.020: "Digital cellular telecommunications system (Phase 2+); Security related network functions".

[8] void

[9] 3GPP TS 51.011: " Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[10] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[11] ITU-T Recommendation E.212: "The international identification plan for public networks and subscriptions ".

[12] ITU-T Recommendation E.213: "Telephone and ISDN numbering plan for land Mobile Stations in public land mobile networks (PLMN)".

[13] ITU-T Recommendation X.121: "International numbering plan for public data networks".

[14] IETF RFC 791: "Internet Protocol".

[15] IETF RFC 2373: "IP Version 6 Addressing Architecture".

[16] 3GPP TS 25.401: "UTRAN Overall Description".

[17] 3GPP TS 25.413: "UTRAN Iu Interface RANAP Signalling".

[18] IETF RFC 2181: "Clarifications to the DNS Specification".

[19] IETF RFC 1035: "Domain Names - Implementation and Specification".

[20] IETF RFC 1123: "Requirements for Internet Hosts -- Application and Support".

[21] IETF RFC 2462: "IPv6 Stateless Address Autoconfiguration".

[22] IETF RFC 3041: "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

[23] 3GPP TS 23.236: "Intra Domain Connection of RAN Nodes to Multiple CN Nodes".

[24] 3GPP TS 23.228: "IP Multimedia (IM) Subsystem – Stage 2"

[25] Void

[26] IETF RFC 3261: "SIP: Session Initiation Protocol"

[27] 3GPP TS 31.102: "Characteristics of the USIM Application."

[28] Void

[29] 3GPP TS 44.118: "Radio Resource Control (RRC) Protocol, Iu Mode".

[30] Void

[31] 3GPP TS 29.002: "Mobile Application Part (MAP) specification"

[32] 3GPP TS 22.016: "International Mobile Equipment Identities (IMEI)"

[33] Void

[34] Void

[35] 3GPP TS 45.056: "CTS-FP Radio Sub-system"

[36] 3GPP TS 42.009: "Security aspects"

[37] 3GPP TS 25.423: "UTRAN Iur interface RNSAP signalling"

[38] 3GPP TS 25.419: "UTRAN Iu-BC interface: Service Area Broadcast Protocol (SABP)"

[39] 3GPP TS 25.410: "UTRAN Iu Interface: General Aspects and Principles"

[40] ISO/IEC 7812: "Identification cards - Numbering system and registration procedure for issuer identifiers"

[41] Void

[42] 3GPP TS 33.102 "3G security; Security architecture"

[43] 3GPP TS 43.130: "Iur-g interface; Stage 2"

[45] IETF RFC 3966: "The tel URI for Telephone Numbers"

[46] 3GPP TS 44.068: "Group Call Control (GCC) protocol".

[47] 3GPP TS 44.069: "Broadcast Call Control (BCC) Protocol ".

[48] 3GPP TS 24.234 Release 12: "3GPP System to WLAN Interworking; UE to Network protocols; Stage 3".

[49] Void

[50] IETF RFC 4187: "EAP AKA Authentication".

[51] IETF RFC 4186: "EAP SIM Authentication".

[52] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description"

[53] IETF RFC 4282: "The Network Access Identifier".

[54] IETF RFC 2279: "UTF-8, a transformation format of ISO 10646".

[55] 3GPP TS 33.234 Release 12: "Wireless Local Area Network (WLAN) interworking security".

[56] Void

[58] 3GPP TS 33.221 "Generic Authentication Architecture (GAA); Support for Subscriber Certificates".

[60] IEEE 1003.1-2004, Part 1: Base Definitions

[61] 3GPP TS 43.318: "Generic Access to the A/Gb interface; Stage 2"

[62] 3GPP TS 44.318: "Generic Access (GA) to the A/Gb interface; Mobile GA interface layer 3 specification"

[63] 3GPP TS 29.163: "Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks"

[64] IETF RFC 2606: "Reserved Top Level DNS Names"

[65] Void

[66] 3GPP TS 51.011 Release 4: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface"

[67] 3GPP2 X.S0013-004: "IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3"

[68] 3GPP TS 23.402: "Architecture Enhancements for non-3GPP accesses"

[69] 3GPP TS 33.402: "3GPP System Architecture Evolution: Security Aspects of non-3GPP accesses"

[70] 3GPP TS 23.292: "IP Multimedia Subsystem (IMS) Centralized Services; Stage 2"

[71] 3GPP TS 23.237: "IP Multimedia Subsystem (IMS) Service Continuity"

[72] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access"

[73] 3GPP TS 29.303: "Domain Name System Procedures; Stage 3"

[74] IETF RFC 3958: "Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS)"

[75] Void

[76] 3GPP TS 23.237: "Mobility between 3GPP-Wireless Local Area Network (WLAN) interworking and 3GPP systems"

[77] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3"

[78] 3GPP TS 29.273: "Evolved Packet System; 3GPP EPS AAA Interfaces"

[79] IETF RFC 7254: "A Uniform Resource Name Namespace for the Global System for Mobile Communications Association (GSMA) and the International Mobile station Equipment Identity (IMEI)".

[80] IETF RFC 4122: "A Universally Unique IDentifier (UUID) URN Namespace".

[81] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[82] IETF RFC5448: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA') "

[83] 3GPP TS 22.011: "Service accessibility".

[84] 3GPP TS 36.413: "Evolved Universal Terrestrial Radio Access Network (E-UTRAN) ; S1 Application Protocol (S1AP)".

[85] Guidelines for use of a 48-bit Extended Unique Identifier (EUI-48™), http://standards.ieee.org/regauth/oui/tutorials/EUI48.html

[86] GUIDELINES FOR 64-BIT GLOBAL IDENTIFIER (EUI-64) REGISTRATION AUTHORITY, http://standards.ieee.org/regauth/oui/tutorials/EUI64.html

[87] The Broadband Forum TR-069: "CPE WAN Management Protocol v1.1", Issue 1 Amendment 2, December 2007

[88] 3GPP TS 29.274: "Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3".

[89] 3GPP TS 33.401: "3GPP System Architecture Evolution: Security Architecture".

[90] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[91] 3GPP TS 36.300: " Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2".

[92] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SRVCC)".

[93] 3GPP TS 31.103: "IP Multimedia Services Identity Module (ISIM) application".

[94] IETF RFC 4825: "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)".

[95] 3GPP TS 29.229: " Cx and Dx interfaces based on the Diameter protocol; Protocol details".

[96] 3GPP TS 29.329: " Sh Interface based on the Diameter protocol; Protocol details".

[97] 3GPP TS 29.165: "Inter-IMS Network to Network Interface (NNI); Stage 3".

[98] 3GPP TS 23.682: "Architecture Enhancements to facilitate communications with Packet Data Networks and Applications".

[99] 3GPP TS 44.018: "Mobile radio interface layer 3 specification; Radio Resource Control (RRC) protocol".

[100] 3GPP TS 44.060: "General Packet Radio Service (GPRS); Mobile Station (MS) – Base Station System (BSS) interface; Radio Link Control / Medium Access Control (RLC/MAC) protocol".

[101] 3GPP TS 23.251: "Network Sharing; Architecture and functional description".

[102] 3GPP TS 32.508: "Procedure flows for multi-vendor plug-and-play eNB connection to the network".

[103] 3GPP TS 23.303: "Proximity-based services (ProSe)".

[104] IETF RFC 7255: "Using the International Mobile station Equipment Identity (IMEI) Uniform Resource Name (URN) as an Instance ID".

[105] 3GPP TS 26.346: "Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs".

[106] 3GPP TS 29.212: "Policy and Charging Control (PCC); Reference points".

[107] 3GPP TS 23.203: "Policy and charging control architecture".

[108] 3GPP TS 29.272: "Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol".

[110] Void.

[111] 3GPP TS 24.379: "Mission Critical Push To Talk (MCPTT) call control Protocol specification".

[112] 3GPP TS 43.064: "General Packet Radio Service (GPRS); Overall description of the GPRS Radio Interface; Stage 2".

[113] IETF RFC 6696: "EAP Extensions for the EAP Re-authentication Protocol (ERP)".

[114] 3GPP TS 23.280: "Common functional architecture to support mission critical services".

[115] 3GPP TS 24.281: "Mission Critical Video (MCVideo) signalling control; Protocol specification".

[116] 3GPP TS 24.282: "Mission Critical Data (MCData) signalling control; Protocol specification".

[117] 3GPP TS 23.285: "Architecture enhancements for V2X services".

[118] 3GPP TS 24.116: "Stage 3 aspects of system architecture enhancements for TV services".

[119] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[120] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[121] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System; Stage 2".

[122] ITU-T Recommendation E.101: "Definitions of terms used for identifiers (names, numbers, addresses and other identifiers) for public telecommunication services and networks in the E-series Recommendations".

[123] 3GPP TS 38.413: "NG Radio Access Network (NG-RAN); NG Application Protocol (NGAP)".

[124] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[125] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); stage 3".

[126] IETF RFC 7542: "The Network Access Identifier".

[127] IETF RFC 2818: "HTTP over TLS".

[128] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition; Stage 3".

[129] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".

[130] 3GPP TS 29.510: "5G System; Network Function Repository Services; Stage 3".

1.1.2 Informative references

[44] Void

[57] GSMA PRD IR.34 "Inter-PLMN Backbone Guidelines"

[59] Void

[109] GSMA TS.06 "IMEI Allocation and Approval Process"
http://www.gsma.com/newsroom/gsmadocuments/

1.2 Abbreviations

For the purposes of the present document, the abbreviations defined in 3GPP TS 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

5G-GUTI	5G Globally Unique Temporary Identifier
5GS	5G System
5G-S-TMSI	5G S-Temporary Mobile Subscription Identifier
AMF	Access and Mobility Management Function
EPS	Evolved Packet System
ER	EAP Re-authentication
ERP	EAP Re-authentication Protocol
GUAMI	Globally Unique AMF Identifier
GUTI	Globally Unique Temporary UE Identity
ICS	IMS Centralized Services
MTC	Machine Type Communication
NCGI	NR Cell Global Identity
NCI	NR Cell Identity
OCS	Online Charging System
PEI	Permanent Equipment Identifier

RACS	Radio Capability Signalling Optimisation
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TWAP	Trusted WLAN AAA Proxy
UUID	Universally Unique Identifier
V2X	Vehicle-to-Everything
WebRTC	Web Real-Time Communication
WWSF	WebRTC Web Server Function

1.3 General comments to references

The identification plan for public networks and subscriptions defined below is that defined in ITU-T Recommendation E.212.

The ISDN numbering plan for MSs and the allocation of mobile station roaming numbers is that defined in ITU-T Recommendation E.213. Only one of the principles for allocating ISDN numbers is proposed for PLMNs. Only the method for allocating MS roaming numbers contained in the main text of ITU-T Recommendation E.213 is recommended for use in PLMNs. If there is any difference between the present document and the ITU-T Recommendations, the former shall prevail.

For terminology, see also ITU-T Recommendations E.101, E.164 and X.121.

1.4 Conventions on bit ordering

The following conventions hold for the coding of the different identities appearing in the present document and in other GSM Technical Specifications if not indicated otherwise:

- the different parts of an identity are shown in the figures in order of significance;
- the most significant part of an identity is on the left part of the figure and the least significant on the right.

When an identity appears in other Technical Specifications, the following conventions hold if not indicated otherwise:

- digits are numbered by order of significance, with digit 1 being the most significant;
- bits are numbered by order of significance, with the lowest bit number corresponding to the least significant bit.

2 Identification of mobile subscribers

2.1 General

A unique International Mobile Subscription Identity (IMSI) shall be allocated to each mobile subscriber in the GSM/UMTS/EPS system.

NOTE: This IMSI is the concept referred to by ITU-T as "International Mobile Subscription Identity".

In order to support the subscriber identity confidentiality service the VLRs, SGSNs and MME may allocate Temporary Mobile Subscriber Identities (TMSI) to visiting mobile subscribers. The VLR,SGSN and MME must be capable of correlating an allocated TMSI with the IMSI of the MS to which it is allocated.

An MS may be allocated three TMSIs, one for services provided through the MSC, one for services provided through the SGSN (P-TMSI for short) and one for the services provided via the MME (M-TMSI part GUTI for short).

For addressing on resources used for GPRS, a Temporary Logical Link Identity (TLLI) is used. The TLLI to use is built by the MS either on the basis of the P-TMSI (local or foreign TLLI), or directly (random TLLI).

In order to speed up the search for subscriber data in the VLR a supplementary Local Mobile Station Identity (LMSI) is defined.

The LMSI may be allocated by the VLR at location updating and is sent to the HLR together with the IMSI. The HLR makes no use of it but includes it together with the IMSI in all messages sent to the VLR concerning that MS.

2.2 Composition of IMSI

IMSI is composed as shown in figure 1.

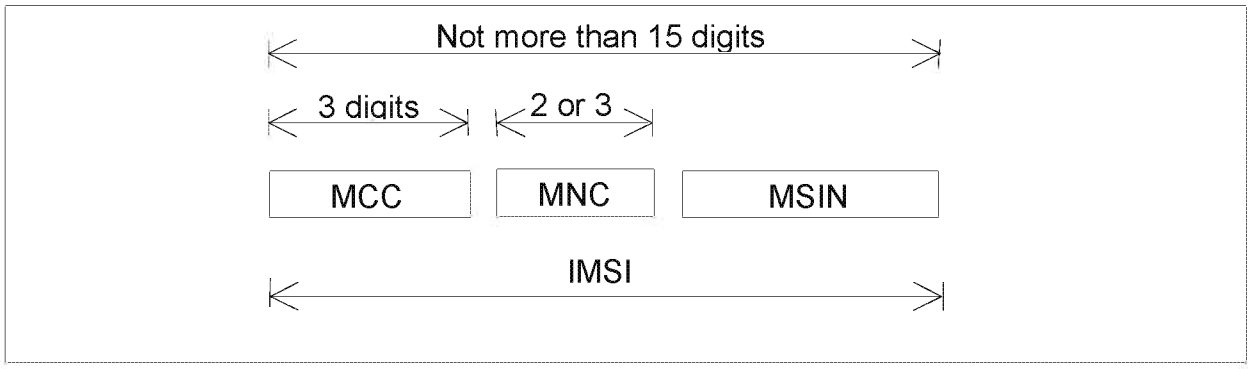

Figure 1: Structure of IMSI

IMSI is composed of three parts:

1) Mobile Country Code (MCC) consisting of three digits. The MCC identifies uniquely the country of domicile of the mobile subscription;

2) Mobile Network Code (MNC) consisting of two or three digits for 3GPP network applications. The MNC identifies the home PLMN of the mobile subscription. The length of the MNC (two or three digits) depends on the value of the MCC. A mixture of two and three digit MNC codes within a single MCC area is not recommended and is outside the scope of this specification.

3) Mobile Subscriber Identification Number (MSIN) identifying the mobile subscription within a PLMN.

2.2A Subscription Permanent Identifier (SUPI)

The SUPI is a globally unique 5G Subscription Permanent Identifier allocated to each subscriber in the 5G System. It is defined in clause 5.9.2 of 3GPP TS 23.501 [119].

The SUPI is defined as:

- a SUPI type: in this release of the specification, it may indicate an IMSI or a network specific identifier; and
- dependent on the value of the SUPI type:
  - an IMSI as defined in clause 2.1; or
  - a network specific identifier, taking the form of a Network Access Identifier (NAI) as defined in clause 28.7.2.

NOTE: Depending on the protocol used to convey the SUPI, the SUPI type can take different formats.

2.2B Subscription Concealed Identifier (SUCI)

The SUCI is a privacy preserving identifier containing the concealed SUPI. It is defined in clause 6.12.2 of 3GPP TS 33.501 [124].

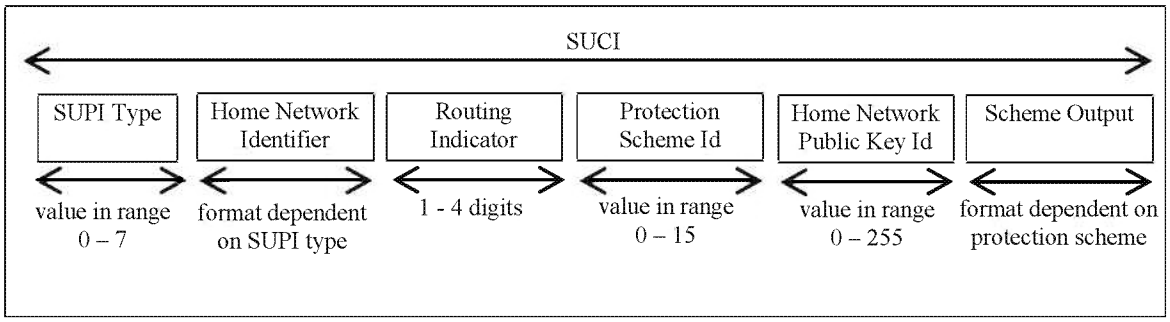

Figure 2.2B-1: Structure of SUCI

The SUCI is composed of the following parts:

1) SUPI Type, consisting in a value in the range 0 to 7. It identifies the type of the SUPI concealed in the SUCI. The following values are defined:

   - 0: IMSI
   - 1: Network Specific Identifier
   - 2 to 7: spare values for future use.

2) Home Network Identifier, identifying the home network of the subscriber.

   When the SUPI Type is an IMSI, the Home Network Identifier is composed of two parts:

   - Mobile Country Code (MCC), consisting of three decimal digits. The MCC identifies uniquely the country of domicile of the mobile subscription;
   - Mobile Network Code (MNC), consisting of two or three decimal digits. The MNC identifies the home PLMN of the mobile subscription.

   When the SUPI type is a Network Specific Identifier, the Home Network Identifier consists of a string of characters with a variable length representing a domain name as specified in clause 2.2 of IETF RFC 7542 [126].

3) Routing Indicator, consisting of 1 to 4 decimal digits assigned by the home network operator and provisioned in the USIM, that allow together with the Home Network Identifier to route network signalling with SUCI to AUSF and UDM instances capable to serve the subscriber.

   Each decimal digit present in the Routing Indicator shall be regarded as meaningful (e.g. value "012" is not the same as value "12"). If no Routing Indicator is configured on the USIM, this data field shall be set to the value 0 (i.e. only consist of one decimal digit of "0").

4) Protection Scheme Identifier, consisting in a value in the range of 0 to 15 (see Annex C.1 of 3GPP TS 33.501 [124]). It represents the null-scheme or a non-null-scheme specified in Annex C of 3GPP TS 33.501 [124] or a protection scheme specified by the HPLMN;

5) Home Network Public Key Identifier, consisting in a value in the range 0 to 255. It represents a public key provisioned by the HPLMN and it is used to identify the key used for SUPI protection. In case of null-scheme being used, this data field shall be set to the value 0;

6) Scheme Output, consisting of a string of characters with a variable length or hexadecimal digits, dependent on the used protection scheme, as defined below. It represents the output of a public key protection scheme specified in Annex C of 3GPP TS 33.501 [124] or the output of a protection scheme specified by the HPLMN.

Figure 2.2B-2 defines the scheme output for the null-scheme.

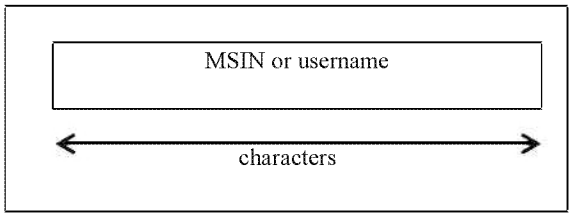

Figure 2.2B-2: Scheme Output for the null-scheme

The Mobile Subscriber Identification Number (MSIN) as defined in clause 2.2 or the username identifies the mobile subscription within the Home Network. The scheme output is formatted as a variable length of characters as specified for the username in clause 2.2 of IETF RFC 7542 [126].

NOTE: If the null-scheme is used, the NFs can derive SUPI from SUCI when needed. The AMF derives SUPI used for AUSF discovery from SUCI when the Routing-Indicator is zero and the Protection Scheme is null-scheme.

Figure 2.2B-3 defines the scheme output for the Elliptic Curve Integrated Encryption Scheme Profile A.

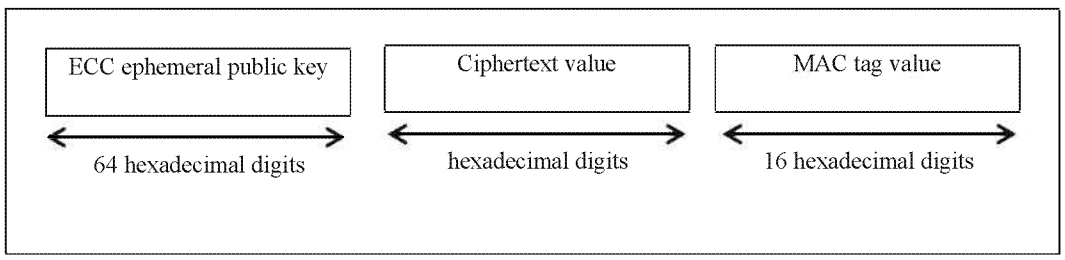

Figure 2.2B-3: Scheme Output for Elliptic Curve Integrated Encryption Scheme Profile A

The ECC ephemeral public key is formatted as 64 hexadecimal digits, which allows to encode 256 bits.

The ciphertext value is formatted as a variable length of hexadecimal digits.

The MAC tag value is formatted as 16 hexadecimal digits, which allows to encode 64 bits.

Editor's Note: clause C.3.2 of TS 33.501 specifies that the scheme output may contain other parameters (not further defined in the specification). It is FFS how to format these parameters.

Figure 2.2B-4 defines the scheme output for the Elliptic Curve Integrated Encryption Scheme Profile B.

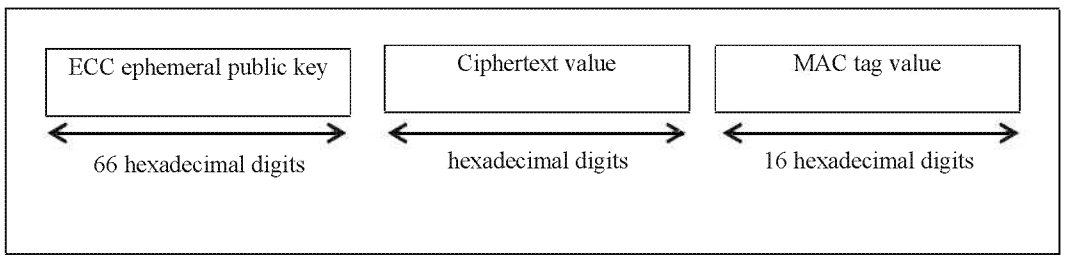

Figure 2.2B-4: Scheme Output for Elliptic Curve Integrated Encryption Scheme Profile B

The ECC ephemeral public key is formatted as 66 hexadecimal digits, which allows to encode 264 bits.

The ciphertext value is formatted as a variable length of hexadecimal digits.

The MAC tag value is formatted as 16 hexadecimal digits, which allows to encode 64 bits.

Editor's Note: clause C.3.2 of TS 33.501 specifies that the scheme output may contain other parameters (not further defined in the specification). It is FFS how to format these parameters.

Figure 2.2B-5 defines the scheme output for HPLMN proprietary protection schemes.

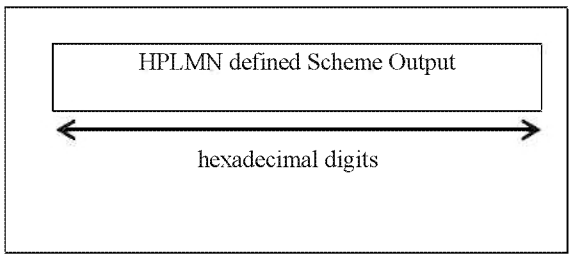

Figure 2.2B-5: Scheme Output for HPLMN proprietary protection schemes

The HPLMN defined scheme output is formatted as a variable length of hexadecimal digits. Its format is not further defined in 3GPP specifications.

As examples, assuming the IMSI 234150999999999, where MCC=234, MNC=15 and MSISN=0999999999, the Routing Indicator 678, and a Home Network Public Key Identifier of 27:

- the SUCI for the null-scheme is composed of: 0, 234, 15, 678, 0, 0 and 0999999999
- the SUCI for the Profile <A> protection scheme is composed of: 0, 234, 15, 678, 1, 27, <EEC ephemeral public key value>, <encryption of 0999999999> and <MAC tag value>

2.3 Allocation and assignment principles

IMSI shall consist of decimal digits (0 through 9) only.

The number of digits in IMSI shall not exceed 15.

The allocation and assignment of Mobile Country Codes (MCCs) is administered by the ITU. The current assignment is available on ITU web site (https://www.itu.int/en/ITU-T/inr/Pages/default.aspx).

The assignment of Mobile network Codes (MNC) is the responsibility of each national numbering plan administrator. MNCs under MCC ranges 90x are administered by the ITU. The MSIN is the third field of the IMSI, and is administered by the relevant MNC assignee to identify individual subscriptions.

If more than one PLMN exists in a country, the same Mobile Network Code should not be assigned to more than one PLMN.

The allocation of IMSIs should be such that not more than the digits MCC + MNC of the IMSI have to be analysed in a foreign PLMN for information transfer.

2.4 Structure of TMSI

Since the TMSI has only local significance (i.e. within a VLR and the area controlled by a VLR, or within an SGSN and the area controlled by an SGSN, or within an MME and the area controlled by an MME), the structure and coding of it can be chosen by agreement between operator and manufacturer in order to meet local needs.

The TMSI consists of 4 octets. It can be coded using a full hexadecimal representation.

In order to avoid double allocation of TMSIs after a restart of an allocating node, some part of the TMSI may be related to the time when it was allocated or contain a bit field which is changed when the allocating node has recovered from the restart.

In areas where both MSC-based services and SGSN-based services are provided, some discrimination is needed between the allocation of TMSIs for MSC-based services and the allocation of TMSIs for SGSN-based services. The discrimination shall be done on the 2 most significant bits, with values 00, 01, and 10 being used by the VLR, and 11 being used by the SGSN.

If intra domain connection of RAN nodes to multiple CN nodes as described in 3GPP TS 23.236 [23] is applied in the MSC/VLR or SGSN, then the NRI shall be part of the TMSI. The NRI has a configurable length of 0 to 10 bits. A configurable length of 0 bits indicates that the NRI is not used and this feature is not applied in the MSC/VLR or SGSN. The NRI shall be coded in bits 23 to 14. An NRI shorter than 10 bits shall be encoded with the most significant bit of the NRI field in bit 23.

The TMSI shall be allocated only in ciphered form. See also 3GPP TS 43.020 [7] and 3GPP TS 33.102 [42].

The network shall not allocate a TMSI with all 32 bits equal to 1 (this is because the TMSI must be stored in the SIM, and the SIM uses 4 octets with all bits equal to 1 to indicate that no valid TMSI is available).

To allow for eventual modifications of the management of the TMSI code space management, MSs shall not check if an allocated TMSI belongs to the range allocated to the allocating node. MSs shall use an allocated TMSI according to the specifications, whatever its value.

2.5 Structure of LMSI

The LMSI consists of 4 octets and may be allocated by the VLR. The VLR shall not allocate the value zero. The value zero is reserved to indicate that an LMSI parameter sent from the HLR to the VLR shall not be interpreted.

2.6 Structure of TLLI

A TLLI is built by the MS or by the SGSN either on the basis of the P-TMSI (local or foreign TLLI), or directly (random or auxiliary TLLI), according to the following rules.

The TLLI consists of 32 bits, numbered from 0 to 31 by order of significance, with bit 0 being the LSB.

A local TLLI is built by an MS which has a valid P-TMSI as follows:

bits 31 down to 30 are set to 1; and

bits 29 down to 0 are set equal to bits 29 to 0 of the P-TMSI.

A foreign TLLI is built by an MS which has a valid P-TMSI as follows:

bit 31 is set to 1 and bit 30 is set to 0; and

bits 29 down to 0 are set equal to bits 29 to 0 of the P-TMSI.

A random TLLI is built by an MS as follows:

bit 31 is set to 0;

bits 30 down to 27 are set to 1; and

bits 0 to 26 are chosen randomly.

An auxiliary TLLI is built by the SGSN as follows:

bit 31 is set to 0;

bits 30 down to 28 are set to 1;

bit 27 is set to 0; and

bits 0 to 26 can be assigned independently.

Other types of TLLI may be introduced in the future.

Part of the TLLI codespace is re-used in GERAN to allow for the inclusion of the GERAN Radio Network Temporary Identifier in RLC/MAC messages. The G-RNTI is defined in 3GPP TS 44.118 [29].

The structure of the TLLI is summarised in table 1.

Table 1: TLLI structure

31	30	29	28	27	26 to 0	Type of TLLI
1	1	T	T	T	T	Local TLLI
1	0	T	T	T	T	Foreign TLLI
0	1	1	1	1	R	Random TLLI
0	1	1	1	0	A	Auxiliary TLLI
0	1	1	0	X	X	Reserved
0	1	0	X	X	X	Reserved
0	0	0	0	G	G	Part of the assigned G-RNTI
0	0	0	1	R	R	Random G-RNTI

'T', 'R', 'A' and 'X' indicate bits which can take any value for the type of TLLI. More precisely, 'T' indicates bits derived from a P-TMSI, 'R' indicates bits chosen randomly, 'A' indicates bits chosen by the SGSN, 'G' indicates bits derived from the assigned G-RNTI and 'X' indicates bits in reserved ranges.

2.7 Structure of P-TMSI Signature

The P-TMSI Signature consists of 3 octets and may be allocated by the SGSN.

The network shall not allocate a P-TMSI Signature with all 24 bits equal to 1 (this is because the P-TMSI Signature must be stored in the SIM, and the SIM uses 3 octets with all bits equal to 1 to indicate that no valid P-TMSI signature is available.

2.8 Globally Unique Temporary UE Identity (GUTI)

2.8.1 Introduction

The purpose of the GUTI is to provide an unambiguous identification of the UE that does not reveal the UE or the user's permanent identity in the Evolved Packet System (EPS). It also allows the identification of the MME and network. It can be used by the network and the UE to establish the UE's identity during signalling between them in the EPS. See 3GPP TS 23.401 [72].

The GUTI has two main components:

- one that uniquely identifies the MME which allocated the GUTI; and
- one that uniquely identifies the UE within the MME that allocated the GUTI.

Within the MME, the mobile shall be identified by the M-TMSI.

The Globally Unique MME Identifier (GUMMEI) shall be constructed from the MCC, MNC and MME Identifier (MMEI).

The MMEI shall be constructed from an MME Group ID (MMEGI) and an MME Code (MMEC).

The GUTI shall be constructed from the GUMMEI and the M-TMSI.

For paging purposes, the mobile is paged with the S-TMSI. The S-TMSI shall be constructed from the MMEC and the M-TMSI.

The operator shall need to ensure that the MMEC is unique within the MME pool area and, if overlapping pool areas are in use, unique within the area of overlapping MME pools.

NOTE: In some network sharing cases it is required that the MMEC and NRI values are coordinated between the sharing operators, as described in 3GPP TS 23.251 [101]. In order to achieve CS/PS coordination in shared GERAN/UTRAN networks, the MMEC included in the GUTI can be set to identify the CS operator serving the UE.

The GUTI shall be used to support subscriber identity confidentiality, and, in the shortened S-TMSI form, to enable more efficient radio signalling procedures (e.g. paging and Service Request).

The format and size of the GUTI is therefore the following:

<GUTI> = <GUMMEI><M-TMSI>,

where <GUMMEI> = <MCC><MNC><MME Identifier>

and <MME Identifier> = <MME Group ID><MME Code>

MCC and MNC shall have the same field size as in earlier 3GPP systems.

M-TMSI shall be of 32 bits length.

MME Group ID shall be of 16 bits length.

MME Code shall be of 8 bits length.

2.8.2 Mapping between Temporary and Area Identities for the EUTRAN and the UTRAN/GERAN based systems

2.8.2.0 Introduction

This clause provides information on the mapping of the temporary and location area identities, e.g. for the construction of the Routeing Area Update Request message in GERAN/UTRAN or Tracking Area Update Request message in E-UTRAN.

In GERAN and UTRAN:

<RAI> = <MCC><MNC><LAC><RAC>

<P-TMSI/TLLI> includes the mapped NRI

P-TMSI shall be of 32 bits length where the two topmost bits are reserved and always set to '11'. Hence, for a UE which may handover to GERAN/UTRAN (based on subscription and UE capabilities), the corresponding bits in the M-TMSI are set to '11' (see clause 2.8.2.1.3).

3GPP TS 23.236 [23] specifies that the NRI field is of variable length and shall be mapped into the P-TMSI starting at bit 23 and down to bit 14. The most significant bit of the NRI is located at bit 23 of the P-TMSI regardless of the configured length of the NRI. To support mobility between GERAN/UTRAN and E-UTRAN, the NRI length is limited to a maximum of 8 bits to be compatible for the mapping to MME Code within GUTI (see clause 2.8.2.2).

The P-TMSI and NRI are defined elsewhere in this specification.

In the case of a combined MME-SGSN node, the NRI of the SGSN part and the MME code of the MME part, refer to the same combined node. RAN configuration allows NAS messages on GERAN/UTRAN and E-UTRAN to be routed to the same combined node. The same or different values of NRI and MME code may be used for a combined node.

2.8.2.1 Mapping from GUTI to RAI, P-TMSI and P-TMSI signature

2.8.2.1.1 Introduction

This clause addresses the case when a UE moves from an MME to an SGSN. The SGSN may be either an S4 SGSN or a Gn/Gp SGSN.

2.8.2.1.2 Mapping in the UE

When a UE moves from an E-UTRAN to a GERAN/UTRAN, the UE needs to map the GUTI to an RAI, a P-TMSI and a P-TMSI Signature, for them to be sent to the SGSN. For GERAN, the TLLI is derived from the P-TMSI by the UE and is a foreign TLLI (see clause 2.6).

The mapping of the GUTI shall be done to the combination of RAI of GERAN / UTRAN and the P-TMSI:

E-UTRAN <MCC> maps to GERAN/UTRAN <MCC>

E-UTRAN <MNC> maps to GERAN/UTRAN <MNC>

E-UTRAN <MME Group ID> maps to GERAN/UTRAN <LAC>

E-UTRAN <MME Code> maps to GERAN/UTRAN <RAC> and is also copied into the 8 Most Significant Bits of the NRI field within the P-TMSI;

E-UTRAN <M-TMSI> maps as follows:

- 6 bits of the E-UTRAN <M-TMSI> starting at bit 29 and down to bit 24 are mapped into bit 29 and down to bit 24 of the GERAN/UTRAN <P-TMSI>;
- 16 bits of the E-UTRAN <M-TMSI> starting at bit 15 and down to bit 0 are mapped into bit 15 and down to bit 0 of the GERAN/UTRAN <P-TMSI>;
- and the remaining 8 bits of the E-UTRAN <M-TMSI> are mapped into the 8 Most Significant Bits of the <P-TMSI signature> field.

The UE shall fill the remaining 2 octets of the <P-TMSI signature> according to clauses 9.1.1, 9.4.1, 10.2.1, or 10.5.1 of 3GPP TS.33.401 [89] , as appropriate, for RAU/Attach procedures.

For UTRAN, the 10-bit long NRI bits are masked out from the P-TMSI and are also supplied by the UE to the RAN node as IDNNS (Intra Domain NAS Node Selector) (see 3GPP TS 23.236 [23]). However, the RAN configured NRI length should not exceed 8 bits.

2.8.2.1.3 Mapping in the old MME

A new SGSN attempts to retrieve information regarding the UE, e.g. the IMSI, from the old MME. In order to find the UE context, the MME needs to map the RAI, P-TMSI (or TLLI) and the P-TMSI Signature (sent by the SGSN) to create the GUTI and compare it with the stored GUTI.

The MME shall perform a reverse mapping to the mapping procedure specified in clause 2.8.2.1.2 "Mapping in the UE" (see 3GPP TS 29.060 [6] and 3GPP TS 29.274 [88] for specifics of the messaging). For the reverse mapping, the E-UTRAN <MME Code> within the GUTI shall be set either to bits 23 to 16 of the GERAN/UTRAN <P-TMSI> (i.e., the NRI field) or to the GERAN/UTRAN <RAC>. For GERAN TLLI, the old MME replaces the two topmost bits of TLLI, received from new SGSN via GTPv1, with '11' before mapping the TLLI to the GUTI used for looking up the "UE Context".

2.8.2.2 Mapping from RAI and P-TMSI to GUTI

2.8.2.2.1 Introduction

This clause addresses the case when a UE moves from an SGSN to an MME (i.e. during a TAU or an Attach to MME). The SGSN may be either an S4 SGSN or a Gn/Gp SGSN.

2.8.2.2.2 Mapping in the UE

When the UE moves from the GERAN/UTRAN to the E-UTRAN, the UE needs to map the RAI and P-TMSI to a GUTI to be sent to the MME. The P-TMSI signature is sent intact to the MME.

The mapping of P-TMSI (TLLI) and RAI in GERAN/UTRAN to GUTI in E-UTRAN shall be performed as follows:

GERAN/UTRAN <MCC> maps to E-UTRAN <MCC>

GERAN/UTRAN <MNC> maps to E-UTRAN <MNC>

GERAN/UTRAN <LAC> maps to E-UTRAN <MME Group ID>

GERAN/UTRAN <RAC> maps into bit 23 and down to bit 16 of the M-TMSI

The 8 most significant bits of GERAN/UTRAN <NRI> map to the MME code.

GERAN/UTRAN <P-TMSI> maps as follows:

- 6 bits of the GERAN/UTRAN <P-TMSI> starting at bit 29 and down to bit 24 are mapped into bit 29 and down to bit 24 of the E-UTRAN <M-TMSI>;
- 16 bits of the GERAN/UTRAN <P-TMSI> starting at bit 15 and down to bit 0 are mapped into bit 15 and down to bit 0 of the E-UTRAN <M-TMSI>.

The values of <LAC> and <MME group id> shall be disjoint, so that they can be differentiated.

The most significant bit of the <LAC> shall be set to zero; and the most significant bit of <MME group id> shall be set to one. Based on this definition, the most significant bit of the <MME group id> can be used to distinguish the node type, i.e. whether it is an MME or SGSN. The UE copies the received old SGSN's <LAC> into the <MME Group ID> when sending a message to an MME, regardless of the value of the most significant bit of the <LAC>.
In networks where this definition is not applied (e.g. in networks already configured with LAC with the most significant bit set to 1 before LTE deployment), the information in the TAU/RAU request indicating whether the provided GUTI/P-TMSI is "native" (i.e. no system change) or "mapped" (i.e. system change) can be used to distinguish the node type for UEs implemented according to this release of the specification (see 3GPP TS 24.301 [90] and 3GPP TS 24.008 [5]). Specific network implementations still satisfying 3GPP standard interfaces can be used for pre-Rel-10 UEs to distinguish the node type.

NOTE 1: As an example, at NAS level, the MME/SGSN can retrieve the old SGSN/MME by using additional GUTI/additional RAI/P-TMSI with double DNS query to solve the first time the UE moves between E-UTRAN and GERAN/UTRAN. As another example, the MME/SGSN can retrieve the old SGSN/MME by using double DNS query.

2.8.2.2.3 Mapping in the new MME

In order to retrieve the UE's information, e.g. the IMSI, from the old SGSN, the new MME extracts only the RAI and P-TMSI from the GUTI via the reverse mapping procedure to that specified in clause 2.8.2.2.2. This is done in order to be able to include the mapped RAI and P-TMSI, along with the P-TMSI Signature received by the MME from the UE, in the corresponding message sent to the old SGSN (see 3GPP TS 29.060 [6] and 3GPP TS 29.274 [88] for specifics of the messaging). The old SGSN compares the received RAI, P-TMSI and P-TMSI Signature with the stored values for identifying the UE.

2.9 Structure of the S-Temporary Mobile Subscriber Identity (S-TMSI)

The S-TMSI is the shortened form of the GUTI to enable more efficient radio signalling procedures (e.g. paging and Service Request). For paging purposes, the mobile is paged with the S-TMSI. The S-TMSI shall be constructed from the MMEC and the M-TMSI:

<S-TMSI> = <MMEC><M-TMSI>

See clause 2.8 for these definitions and the mapping.

2.10 5G Globally Unique Temporary UE Identity (5G-GUTI)

2.10.1 Introduction

The purpose of the 5G-GUTI is to provide an unambiguous identification of the UE that does not reveal the UE or the user's permanent identity in the 5G System (5GS). It also allows the identification of the Access and Mobility Management Function (AMF) and network. It can be used by the network and the UE to establish the UE's identity during signalling between them in the 5GS. See 3GPP TS 23.501 [119].

The 5G-GUTI has two main components:

- one that identifies the AMF(s) which allocated the 5G-GUTI; and
- one that uniquely identifies the UE within the AMF(s) that allocated the 5G-GUTI.

Within the AMF(s), the mobile shall be identified by the 5G-TMSI.

The Globally Unique AMF Identifier (GUAMI) shall be constructed from the MCC, MNC and AMF Identifier (AMFI).

The AMFI shall be constructed from an AMF Region ID, an AMF Set ID and an AMF Pointer. The AMF Region ID identifies the region, the AMF Set ID uniquely identifies the AMF Set within the AMF Region, and the AMF Pointer identifies one or more AMFs within the AMF Set.

NOTE: When the UE is assigned a 5G-GUTI with an AMF Pointer value used by more than one AMF, the AMFs need to ensure that the 5G-TMSI value used within the assigned 5G-GUTI is not already in use within the AMF's sharing that pointer value.

The 5G-GUTI shall be constructed from the GUAMI and the 5G-TMSI.

For paging purposes, the mobile is paged with the 5G-S-TMSI. The 5G-S-TMSI shall be constructed from the AMF Set ID, the AMF Pointer and the 5G-TMSI.

The operator shall need to ensure that the combination of the AMF Set ID and AMF Pointer is unique within the AMF Region and, if overlapping AMF Regions are in use, unique within the area of overlapping AMF Regions.

The 5G-GUTI shall be used to support subscriber identity confidentiality, and, in the shortened 5G-S-TMSI form, to enable more efficient radio signalling procedures (e.g. paging and Service Request).

The format and size of the 5G-GUTI is therefore the following:

<5G-GUTI> = <GUAMI><5G-TMSI>,

where <GUAMI> = <MCC><MNC><AMF Identifier>

and <AMF Identifier> = <AMF Region ID><AMF Set ID><AMF Pointer>

MCC and MNC shall have the same field size as in earlier 3GPP systems.

5G-TMSI shall be of 32 bits length.

AMF Region ID shall be of 8 bits length.

AMF Set ID shall be of 10 bits length.

AMF Pointer shall be of 6 bits length.

2.10.2 Mapping between Temporary Identities for the 5GS and the E-UTRAN

2.10.2.0 Introduction

This clause provides information on the mapping of the temporary identities, e.g. for the construction of the Tracking Area Update Request message in E-UTRAN.

In E-UTRAN:

<GUTI> = <MCC><MNC><MME Group ID><MME Code><M-TMSI>

2.10.2.1 Mapping from 5G-GUTI to GUTI

2.10.2.1.1 Introduction

This clause addresses the case when a UE moves from an AMF to an MME.

2.10.2.1.2 Mapping in the UE

When a UE moves from 5GS to an E-UTRAN, the UE needs to map the 5G-GUTI to a GUTI.

The mapping of the 5G-GUTI to a GUTI shall be done as follows:

5GS <MCC> maps to E-UTRAN <MCC>

5GS <MNC> maps to E-UTRAN <MNC>

5GS <AMF Region ID> and 5GS <AMF Set ID> map to E-UTRAN <MME Group ID> and part of E-UTRAN <MME Code> as follows:

- 8 bits of the 5GS <AMF Region ID> starting at bit 7 and down to bit 0 are mapped into bit 15 and down to bit 8 of the E-UTRAN <MME Group ID>;
- 8 bits of the 5GS <AMF Set ID> starting at bit 9 and down to bit 2 are mapped into bit 7 and down to bit 0 of the E-UTRAN <MME Group ID>;
- 2 bits of the 5GS <AMF Set ID> starting at bit 1 and down to bit 0 are mapped into bit 7 and down to bit 6 of the E-UTRAN <MME Code>;

5GS <AMF Pointer> maps to part of E-UTRAN <MME Code> as follows:

- 6 bits of the 5GS <AMF Pointer> starting at bit 5 and down to bit 0 are mapped into bit 5 and down to bit 0 of the E-UTRAN <MME Code>.

5GS <5G-TMSI> maps to to E-UTRAN <M-TMSI>

2.10.2.1.3 Mapping in the old AMF

A new MME attempts to retrieve information regarding the UE, e.g. the IMSI, from the old AMF. In order to find the UE context, the AMF needs to map the GUTI (sent by the MME) to create the 5G-GUTI and compare it with the stored 5G-GUTI.

The AMF shall perform a reverse mapping to the mapping procedure specified in clause 2.10.2.1.2 "Mapping in the UE".

2.10.2.2 Mapping from GUTI to 5G-GUTI

2.10.2.2.1 Introduction

This clause addresses the case when a UE moves from an MME to an AMF (i.e. during a Registration Update or an Initial Registration to an AMF).

2.10.2.2.2 Mapping in the UE

When the UE moves from the E-UTRAN to 5GS, the UE needs to map the GUTI to a 5G-GUTI to be sent to the AMF.

The mapping of the GUTI to a 5G-GUTI shall be performed as follows:

E-UTRAN <MCC> maps to 5GS <MCC>

E-UTRAN <MNC> maps to 5GS <MNC>

E-UTRAN <MME Group ID> maps to 5GS <AMF Region ID> and part of 5GS <AMF Set ID> as follows:

- 8 bits of the E-UTRAN <MME Group ID> starting at bit 15 and down to bit 8 are mapped into bit 7 and down to bit 0 of the 5GS <AMF Region ID>;
- 8 bits of the E-UTRAN <MME Group ID> starting at bit 7 and down to bit 0 are mapped into bit 9 and down to bit 2 of the 5GS <AMF Set ID>;E-UTRAN <MME Code> maps to 5GS <AMF Set ID> and 5GS <AMF Pointer> as follows:
- 2 bits of the E-UTRAN <MME Code> starting at bit 7 and down to bit 6 are mapped into bit 1 and down to bit 0 of the 5GS <AMF Set ID>;
- 6 bits of the E-UTRAN <MMEC Code> starting at bit 5 and down to bit 0 are mapped into bit 5 and down to bit 0 of the 5GS <AMF Pointer >;

E-UTRAN <M-TMSI> maps to 5GS <5G-TMSI>

2.10.2.2.3 Mapping in the new AMF

In order to retrieve the UE's information, e.g. the IMSI, from the old MME, the new AMF shall perform a reverse mapping to the mapping procedure specified in clause 2.10.2.2.2 "Mapping in the UE". This is done in order to be able to include the mapped GUTI in the corresponding message sent to the old MME. The old MME compares the received GUTI with the stored values for identifying the UE.

2.11 Structure of the 5G-S-Temporary Mobile Subscriber Identity (5G-S-TMSI)

The 5G-S-TMSI is the shortened form of the 5G-GUTI to enable more efficient radio signalling procedures (e.g. paging and Service Request). For paging purposes, the mobile is paged with the 5G-S-TMSI. The 5G-S-TMSI shall be constructed from the AMF Set ID, the AMF Pointer and the 5G-TMSI:

<5G-S-TMSI> = <AMF Set ID><AMF Pointer><5G-TMSI>

See clause 2.10.1 for these definitions and clause 2.10.2 for the mapping.

3 Numbering plan for mobile stations

3.1 General

The structure of the following numbers is defined below:

- the telephone number used by a subscriber of a fixed (or mobile) network to call a mobile station of a PLMN;
- the network addresses used for packet data communication between a mobile station and a fixed (or mobile) station;
- mobile station roaming numbers.

One or more numbers of the E.164 numbering plan shall be assigned to a mobile station to be used for all calls to that station, i.e. the assignment of at least one MSISDN (i.e. E.164 number) to a mobile station is mandatory. As an exception, GPRS and EPS allow for operation whereby a MSISDN is not allocated as part of the subscription data (see 3GPP TS 23.060 [3] clause 5.3.17 and 3GPP TS 23.401 [72]).

NOTE: For card operated stations the E.164 number should be assigned to the holder of the card (personal number).

3.2 Numbering plan requirements

In principle, it should be possible for any subscriber of the ISDN or PSTN to call any MS in a PLMN. This implies that E.164 numbers for MSs should comply with the E.164 numbering plan in the home country of the MS.

The E.164 numbers of MSs should be composed in such a way that standard ISDN/PSTN charging can be used for calls to MSs.

It should be possible for each national numbering plan administrator to develop its own independent numbering/addressing plan for MSs.

The numbering/addressing plan should not limit the possibility for MSs to roam among PLMNs.

It should be possible to change the IMSI without changing the E.164 number assigned to an MS and vice versa.

In principle, it should be possible for any subscriber of the CSPDN/PSPDN to call any MS in a PLMN. This implies that it may be necessary for an MS to have a X.121 number.

In principle, it should be possible for any fixed or mobile terminal to communicate with a mobile terminal using an IP v4 address or IP v6 address.

3.3 Structure of Mobile Subscriber ISDN number (MSISDN)

Mobile Subscriber ISDN numbers (i.e. E.164 numbers) are assigned from the E.164 numbering plan [10]; see also ITU-T Recommendation E.213 [12]. The structure of the MSISDN will then be as shown in figure 2.

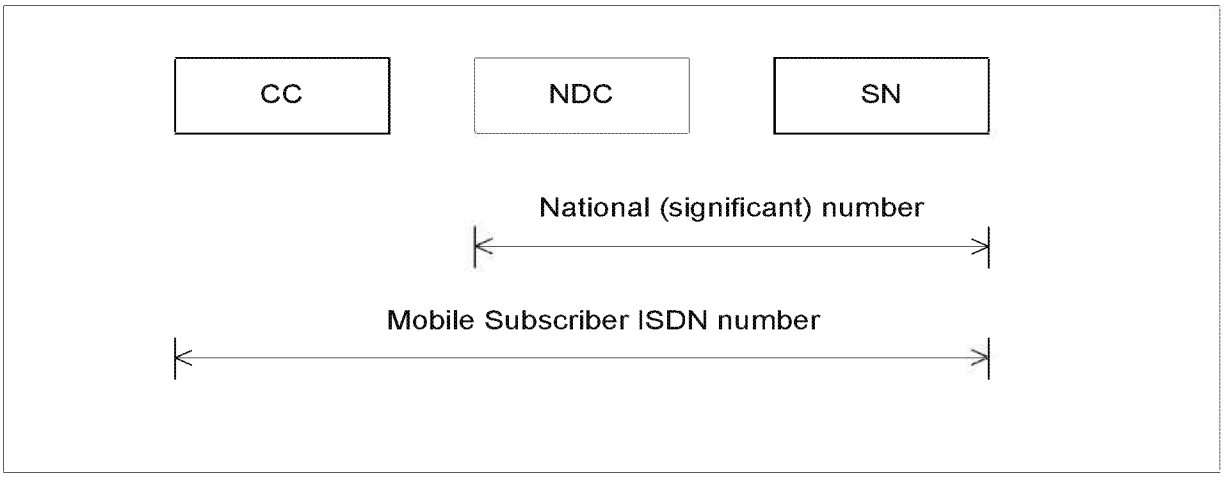

Figure 2: Number Structure of MSISDN

The number consists of:

- Country Code (CC) of the country in which the MS is registered, followed by:
- National (significant) number, which consists of:
  - National Destination Code (NDC) and
  - Subscriber Number (SN).

For GSM/UMTS applications, a National Destination Code is allocated to each PLMN. In some countries more than one NDC may be required for each PLMN/mobile number ranges.

The composition of the MSISDN should be such that it can be used as a global title address in the Signalling Connection Control Part (SCCP) for routeing messages to the home location register of the MS. The country code (CC)

and the national destination code (NDC) will provide such routeing information. If further routeing information is required, it should be contained in the first few digits of the subscriber number (SN).

A sub-address may be appended to an E.164 number for use in call setup and in supplementary service operations where an E.164 number is required (see ITU-T Recommendations E.164, clause Annex B, B.3.3, and X.213 annex A). The sub-address is transferred to the terminal equipment denoted by the ISDN number.

The maximum length of a sub-address is 20 octets, including one octet to identify the coding scheme for the sub-address (see ITU-T Recommendation X.213, annex A). All coding schemes described in ITU-T Recommendation X.213, annex A are supported in 3GPP networks

As an exception to the rules above, the MSISDN shall take the dummy MSISDN value composed of 15 digits set to 0 (encoded as an international E.164 number) when the MSISDN is not available in messages in which the presence of the MSISDN parameter is required for backward compatibility reason. See the relevant stage 3 specifications.

3.4 Mobile Station Roaming Number (MSRN) for PSTN/ISDN routeing

The Mobile Station Roaming Number (MSRN) is used to route calls directed to an MS. On request from the Gateway MSC via the HLR it is temporarily allocated to an MS by the VLR with which the MS is registered; it addresses the Visited MSC collocated with the assigning VLR. More than one MSRN may be assigned simultaneously to an MS.

The MSRN is passed by the HLR to the Gateway MSC to route calls to the MS.

The Mobile Station Roaming Number for PSTN/ISDN routing shall have the same structure as international E.164 numbers in the area in which the roaming number is allocated, i.e.:

- the country code of the country in which the visitor location register is located;
- the national destination code of the visited PLMN or numbering area;
- a subscriber number with the appropriate structure for that numbering area.

The MSRN shall not be used for subscriber dialling. It should be noted that the MSRN can be identical to the MSISDN (clause 3.3) in certain circumstances. In order to discriminate between subscriber generated access to these numbers and re-routeing performed by the network, re-routeing or redirection indicators or other signalling means should be used, if available.

3.5 Structure of Mobile Station International Data Number

The structure of MS international data numbers should comply with the data numbering plan of ITU-T Recommendation X.121 as applied in the home country of the mobile subscriber. Implications for numbering interworking functions which may need to be provided by the PLMN (if the use of X.121 numbers is required) are indicated in 3GPP TS 23.070 [4].

3.6 Handover Number

The handover number is used for establishment of a circuit between MSCs to be used for a call being handed over. The structure of the handover number is the same as the structure of the MSRN. The handover number may be reused in the same way as the MSRN.

3.7 Structure of an IP v4 address

One or more IP address domains may be allocated to each PLMN. The IP v4 address structure is defined in RFC 791 [14].

An IP v4 address may be allocated to an MS either permanently or temporarily during a connection with the network.

3.8 Structure of an IP v6 address

One or more IP address domains could be allocated to each PLMN. The IP v6 address structure is defined in RFC 2373 [15].

An IP v6 address may be allocated to an MS either permanently or temporarily during a connection with the network

If the dynamic IPv6 stateless address autoconfiguration procedure is used, then each PDP context, or group of PDP contexts sharing the same IP address, is assigned a unique prefix as defined in 3GPP TS 23.060 [3].

As described in RFC 2462 [21] and RFC 3041 [22], the MS can change its interface identifier without the GPRS network being aware of the change.

4 Identification of location areas and base stations

4.1 Composition of the Location Area Identification (LAI)

The Location Area Identification shall be composed as shown in figure 3:

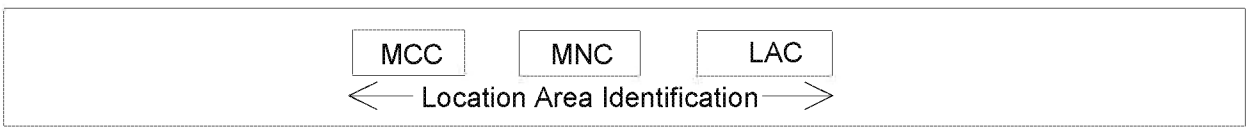

Figure 3: Structure of Location Area Identification

The LAI is composed of the following elements:

- Mobile Country Code (MCC) identifies the country in which the GSM PLMN is located. The value of the MCC is the same as the three digit MCC contained in international mobile subscriber identity (IMSI);
- Mobile Network Code (MNC) is a code identifying the GSM PLMN in that country. The MNC takes the same value as the two or three digit MNC contained in IMSI;
- Location Area Code (LAC) is a fixed length code (of 2 octets) identifying a location area within a PLMN. This part of the location area identification can be coded using a full hexadecimal representation except for the following reserved hexadecimal values:

  0000, and

  FFFE.

  These reserved values are used in some special cases when no valid LAI exists in the MS (see 3GPP TS 24.008 [5], 3GPP TS 31.102 [27] and 3GPP TS 51.011 [9]).

4.2 Composition of the Routing Area Identification (RAI)

The Routing Area Identification shall be composed as shown in figure 4:

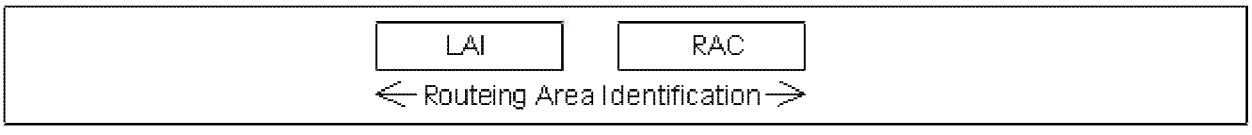

Figure 4: Structure of Routing Area Identification

The RAI is composed of the following elements:

- A valid Location Area Identity (LAI) as defined in clause 4.1. Invalid LAI values are used in some special cases when no valid RAI exists in the mobile station (see 3GPP TS 24.008 [5], 3GPP TS 31.102 [27] and 3GPP TS 51.011 [9]).

- Routeing Area Code (RAC) which is a fixed length code (of 1 octet) identifying a routeing area within a location area.

4.3 Base station identification

4.3.1 Cell Identity (CI) and Cell Global Identification (CGI)

The BSS and cell within the BSS are identified within a location area or routeing area by adding a Cell Identity (CI) to the location area or routeing area identification, as shown in figure 5. The CI is of fixed length with 2 octets and it can be coded using a full hexadecimal representation.

The Cell Global Identification is the concatenation of the Location Area Identification and the Cell Identity. Cell Identity shall be unique within a location area.

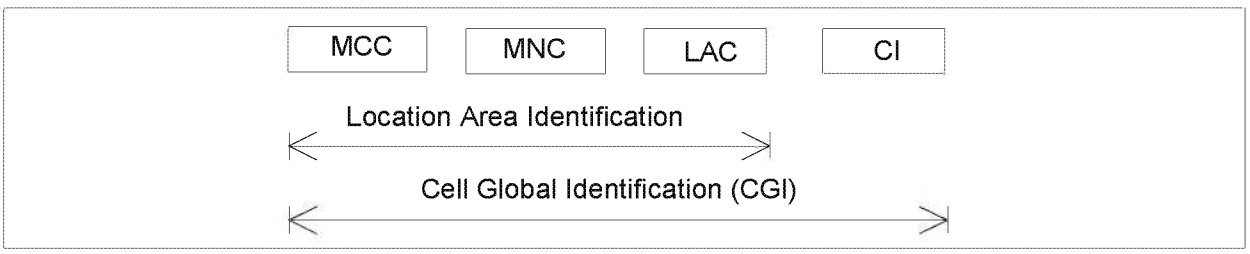

Figure 5: Structure of Cell Global Identification

4.3.2 Base Station Identify Code (BSIC)

The base station identity code is a local colour code that allows an MS to distinguish between different neighbouring base stations. BSIC is a 6 bit code which is structured as shown in Figure 6. Exceptions apply to networks supporting EC-GSM-IoT or PEO and for mobile stations in EC or PEO operation (see 3GPP TS 43.064 [112]) where the BSIC is a 9 bit code which is structured as shown in Figure 6a.

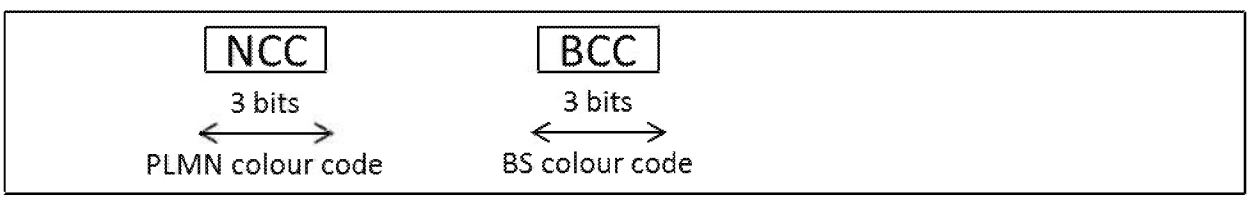

Figure 6: Structure of 6 bit BSIC

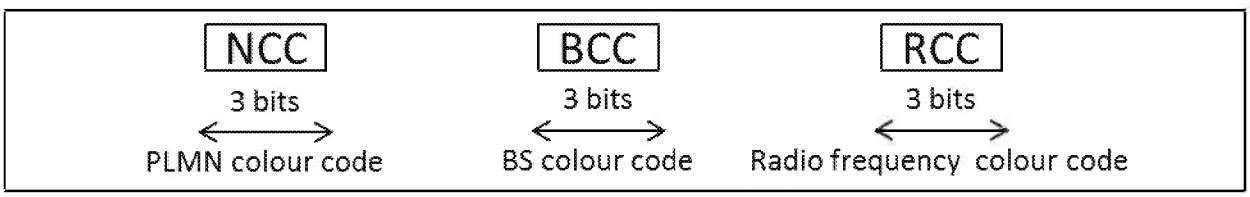

Figure 6a: Structure of 9 bit BSIC

In the definition of the NCC, care should be taken to ensure that the same NCC is not used in adjacent PLMNs which may use the same BCCH carrier frequencies in neighbouring areas. Therefore, to prevent potential deadlocks, a definition of the NCC appears in annex A. This annex will be reviewed in a co-ordinated manner when a PLMN is created.

In addition to the above, the GERAN networks should be configured so that:

- in a cell shared between different PLMNs as per GERAN network sharing (see 3GPP TS 44.018 [99] and 3GPP TS 44.060 [100]), the NCC used in this cell is different from the NCC used in the neighbouring non-shared cells of these PLMNs; and that
- these PLMNs use different NCCs in non-shared cells neighbouring this shared cell.

Furthermore, GERAN networks supporting the 9 bit BSIC shall also support the 6 bit BSIC field and when supporting both the 6 bit BSIC and 9 bit BSIC the network shall ensure that the NCC and BCC parts are identical between the 6 bit and 9 bit BSIC fields.

4.4 Regional Subscription Zone Identity (RSZI)

A PLMN-specific regional subscription defines unambiguously for the entire PLMN the regions in which roaming is allowed. It consists of one or more regional subscription zones. The regional subscription zone is identified by a Regional Subscription Zone Identity (RSZI). A regional subscription zone identity is composed as shown in figure 7.

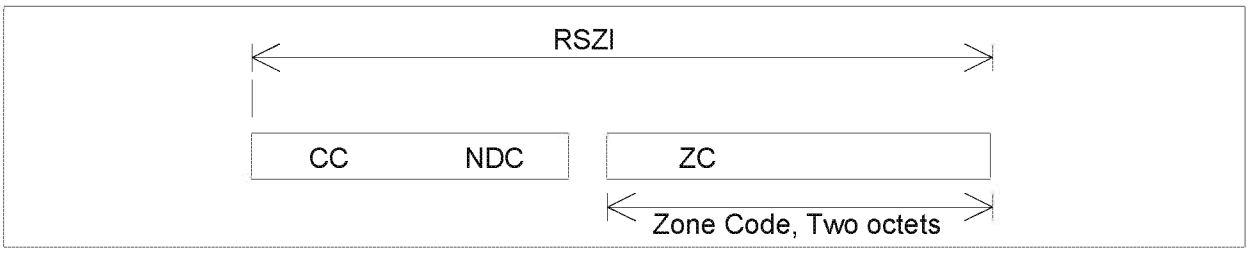

Figure 7: Structure of Regional Subscription Zone Identity (RSZI)

The elements of the regional subscription zone identity are:

1) the Country Code (CC) which identifies the country in which the PLMN is located;
2) the National Destination Code (NDC) which identifies the PLMN in that country;
3) the Zone Code (ZC) which identifies a regional subscription zone as a pattern of allowed and not allowed location areas uniquely within that PLMN.

CC and NDC are those of an ITU-T E.164 VLR or SGSN number (see clause 5.1) of the PLMN; they are coded with a trailing filler, if required. ZC has fixed length of two octets and is coded in full hexadecimal representation.

RSZIs, including the zone codes, are assigned by the VPLMN operator. The zone code is evaluated in the VLR or SGSN by information stored in the VLR or SGSN as a result of administrative action. If a zone code is received by a VLR or SGSN during updating by the HLR and this zone code is related to that VLR or SGSN, the VLR or SGSN shall be able to decide for all its MSC or SGSN areas and all its location areas whether they are allowed or not allowed.

For details of assignment of RSZI and of ZC as subscriber data see 3GPP TS 23.008 [2].

For selection of RSZI at location updating by comparison with the leading digits of the VLR or SGSN number and for transfer of ZC from the HLR to VLR and SGSN see 3GPP TS 29.002 [31].

4.5 Location Number

A location number is a number which defines a specific location within a PLMN. The location number is formatted according to ITU-T Recommendation E.164, as shown in figure 8. The Country Code (CC) and National Destination Code (NDC) fields of the location number are those which define the PLMN of which the location is part.

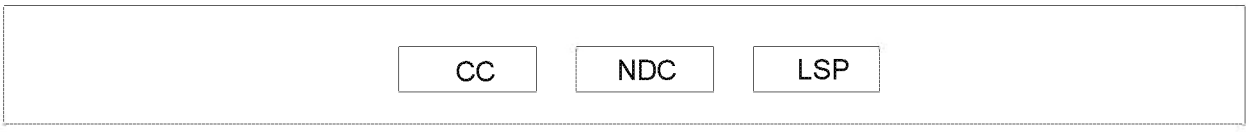

Figure 8: Location Number Structure

The structure of the locally significant part (LSP) of the location number is a matter for agreement between the PLMN operator and the national numbering plan administrator in the PLMN's country. It is desirable that the location number can be interpreted without the need for detailed knowledge of the internal structure of the PLMN; the LSP should therefore include the national destination code in the national numbering plan for the fixed network which defines the geographic area in which the location lies.

The set of location numbers for a PLMN shall be chosen so that a location number can be distinguished from the MSISDN of a subscriber of the PLMN. This will allow the PLMN to trap attempts by users to dial a location number.

4.6 Composition of the Service Area Identification (SAI)

Void (see clause 12.5).

4.7 Closed Subscriber Group

A Closed Subscriber Group consists of a single cell or a collection of cells within an E-UTRAN and UTRAN that are open to only a certain group of subscribers.

Within a PLMN, a Closed Subscriber Group is identified by a Closed Subscriber Group Identity (CSG-ID). The CSG-ID shall be fix length 27 bit value.

4.8 HNB Name

HNB Name shall be a broadcast string in free text format that provides a human readable name for the Home NodeB or Home eNodeB CSG identity.

HNB Name shall be coded in UTF-8 format with variable number of bytes per character. The maximum length of HNB Name shall be 48 bytes.

See 3GPP TS 22.011 [83] for details.

4.9 CSG Type

CSG Type shall provide the type of a CSG identity in a human readable form. It shall reside in the UE only. See 3GPP TS 22.011 [83] for details.

When the CSG Type has a text component, the CSG Type shall be coded in UTF-8 format with variable number of bytes per character . The maximum text length shall not exceed 12 characters in any language.

4.10 HNB Unique Identity

HNB Unique Identity uniquely identifies a Home NodeB or Home eNodeB.

The HNB unique identity shall be defined as either a 48-bit or 64-bit extended unique identifier (EUI-48 or EUI-64) as defined in [45] (EUI-48) and [46] (EUI-64).

For use in HNB certificates, the HNB Unique Identity shall be transformed into a FQDN in the form:

- <EUI-48/64>.<REALM>

<EUI48/64> is the first label which shall be the EUI-48 or EUI-64, represented as a string of 12 or 16 hexadecimal digits including any leading zeros. <REALM> denotes the realm which may consist of 3 labels , e.g. hnb. femtocellvendor.com.

5 Identification of MSCs, GSNs, location registers and CSSs

5.1 Identification for routeing purposes

MSCs, GSNs, location registers and CSSs are identified by international E.164 numbers and/or Signalling Point Codes ("entity number", i.e., "HLR number", "VLR number", "MSC number", "SGSN number", "GGSN number" and "CSS number") in each PLMN.

MMEs that support "SMS in MME" are identified by international PSTN/ISDN numbers for SM Routing via an IWF (i.e. "MME number for MT SMS").

Additionally SGSNs and GGSNs are identified by GSN Addresses. These are the SGSN Address and the GGSN Address.

A GSN Address shall be composed as shown in figure 9.

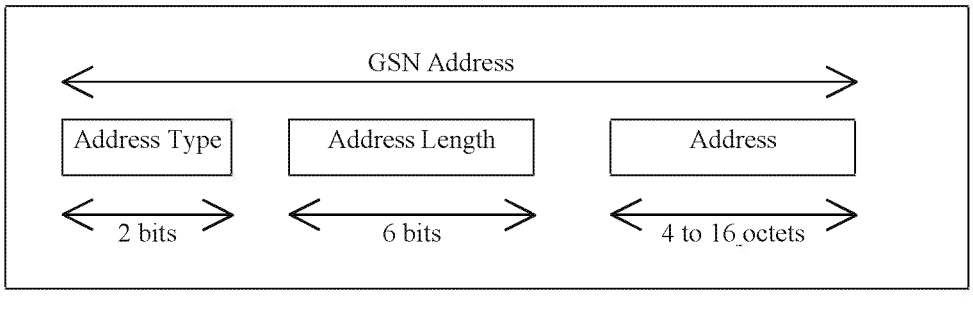

Figure 9: Structure of GSN Address

The GSN Address is composed of the following elements:

1) The Address Type, which is a fixed length code (of 2 bits) identifying the type of address that is used in the Address field.

2) The Address Length, which is a fixed length code (of 6 bits) identifying the length of the Address field.

3) The Address, which is a variable length field which contains either an IPv4 address or an IPv6 address.

Address Type 0 and Address Length 4 are used when Address is an IPv4 address.

Address Type 1 and Address Length 16 are used when Address is an IPv6 address.

The IP v4 address structure is defined in RFC 791 [14].

The IP v6 address structure is defined in RFC 2373 [15].

5.2 Identification of HLR for HLR restoration application

HLR may also be identified by one or several "HLR id(s)", consisting of the leading digits of the IMSI (MCC + MNC + leading digits of MSIN).

5.3 Identification of the HSS for SMS

The HSS may also be identified by a HSS-ID.

The HSS-ID shall consist of decimal digits (0 through 9) only and be composed of the MCC consisting of three digits, the MNC consisting of two or three digits and an index consisting of one to several digits. The number of digits in the HSS-ID shall not exceed 15. This composition is compatible with the IMSI one. The HSS-ID shall not be identical to the complete IMSI of a UE.

NOTE: The composition of the HSS-ID is compatible with the composition of the IMSI in clause 2.2 for routing purposes.

6 International Mobile Station Equipment Identity, Software Version Number and Permanent Equipment Identifier

6.1 General

The structure and allocation principles of the International Mobile station Equipment Identity and Software Version number (IMEISV) and the International Mobile station Equipment Identity (IMEI) are defined below.

The Mobile Station Equipment is uniquely defined by the IMEI or the IMEISV.

6.2 Composition of IMEI and IMEISV

6.2.1 Composition of IMEI

The International Mobile station Equipment Identity (IMEI) is composed as shown in figure 10.

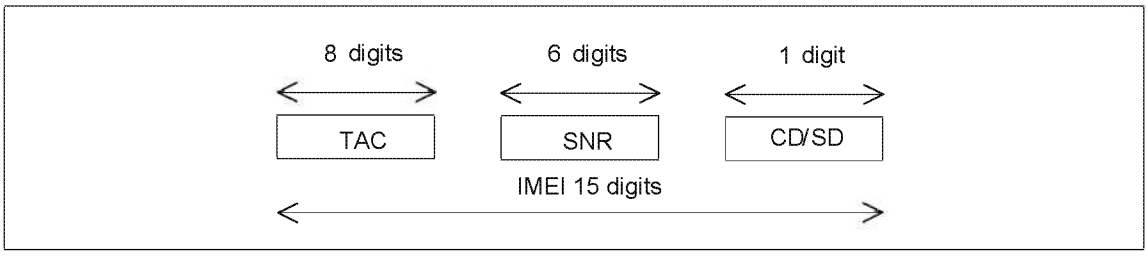

Figure 10: Structure of IMEI

The IMEI is composed of the following elements (each element shall consist of decimal digits only):

- Type Allocation Code (TAC). Its length is 8 digits;
- Serial Number (SNR) is an individual serial number uniquely identifying each equipment within the TAC. Its length is 6 digits;
- Check Digit (CD) / Spare Digit (SD): If this is the Check Digit see paragraph below; if this digit is Spare Digit it shall be set to zero, when transmitted by the MS.

The IMEI (14 digits) is complemented by a Check Digit (CD). The Check Digit is not part of the digits transmitted when the IMEI is checked, as described below. The Check Digit is intended to avoid manual transmission errors, e.g. when customers register stolen MEs at the operator's customer care desk. The Check Digit is defined according to the Luhn formula, as defined in annex B.

NOTE: The Check Digit is not applied to the Software Version Number.

The security requirements of the IMEI are defined in 3GPP TS 22.016 [32].

6.2.2 Composition of IMEISV

The International Mobile station Equipment Identity and Software Version Number (IMEISV) is composed as shown in figure 11.

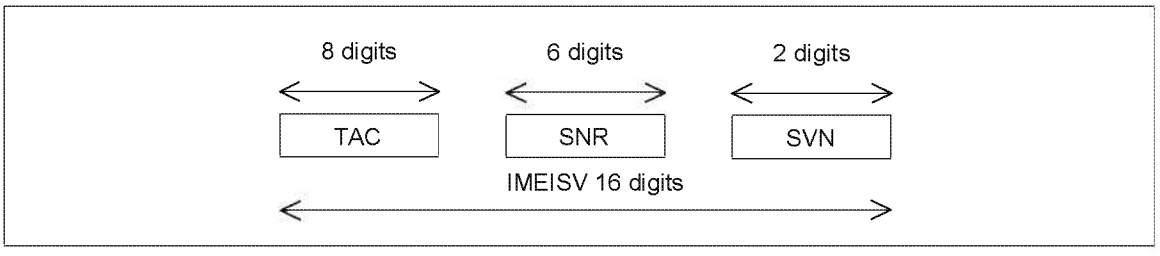

Figure 11: Structure of IMEISV

The IMEISV is composed of the following elements (each element shall consist of decimal digits only):

- Type Allocation Code (TAC). Its length is 8 digits;
- Serial Number (SNR) is an individual serial number uniquely identifying each equipment within each TAC. Its length is 6 digits;
- Software Version Number (SVN) identifies the software version number of the mobile equipment. Its length is 2 digits.

Regarding updates of the IMEISV: The security requirements of 3GPP TS 22.016 [32] apply only to the TAC and SNR, but not to the SVN part of the IMEISV.

6.3 Allocation principles

The Type Allocation Code (TAC) is issued by the GSM Association in its capacity as the Global Decimal Administrator. Further information can be found in the GSMA TS.06 [109] .

Manufacturers shall allocate individual serial numbers (SNR) in a sequential order.

For a given ME, the combination of TAC and SNR used in the IMEI shall duplicate the combination of TAC and SNR used in the IMEISV.

The Software Version Number is allocated by the manufacturer. SVN value 99 is reserved for future use.

6.4 Permanent Equipment Identifier (PEI)

In 5GS, the Permanent Equipment Identifier (PEI) identifies a UE.

The PEI is defined as:

- a PEI type: in this release of the specification, it may indicate an IMEI or IMEISV; and
- dependent on the value of the PEI type:
  - an IMEI as defined in clause 6.2.1; or
  - an IMEISV as defined in clause 6.2.2.

7 Identification of Voice Group Call and Voice Broadcast Call Entities

7.1 Group Identities

Logical groups of subscribers to the Voice Group Call Service or to the Voice Broadcast Service are identified by a Group Identity (Group ID). Group IDs for VGCS are unique within a PLMN. Likewise, Group IDs for VBS are unique within a PLMN. However, no uniqueness is required between the sets of Group IDs. These sets may be intersecting or even identical, at the option of the network operator.

The Group ID is a number with a maximum value depending on the composition of the voice group call reference or voice broadcast call reference defined in clause 7.3.

For definition of Group ID on the radio interface, A interface and Abis interface, see 3GPP TS 44.068 [46] and 3GPP TS 44.069 [47].

For definition of Group ID coding on MAP protocol interfaces, see 3GPP TS 29.002 [31].

VGCS or VBS shall also be provided for roaming. If this applies, certain Group IDs shall be defined as supra-PLMN Group IDs which have to be co-ordinated between the network operators and which shall be known in the networks and in the SIM.

The format of the Group ID is identical for VBS and VGCS.

7.2 Group Call Area Identification

Grouping of cells into specific group call areas occurs in support of both the Voice Group Call Service and the Voice Broadcast Service. These service areas are known by a "Group Call Area Identity" (Group Call Area Id). No restrictions are placed on what cells may be grouped into a given group call area.

The Group Call Area ID is a number uniquely assigned to a group call area in one network and with a maximum value depending on the composition of the voice group call reference or voice broadcast reference defined under 7.3.

The formats of the Group Call Area ID for VGCS and the Group Call Area ID for VBS are identical.

7.3 Voice Group Call and Voice Broadcast Call References

Specific instances of voice group calls (VGCS) and voice broadcast calls (VBS) within a given group call area are known by a "Voice Group Call Reference" or by a "Voice Broadcast Call Reference" respectively.

Each voice group call or voice broadcast call in one network is uniquely identified by its Voice Group Call Reference or Voice Broadcast Call Reference. The Voice Group Call Reference or Voice Broadcast Call Reference is composed of the Group ID and the Group Call Area ID. The composition of the group call area ID and the group ID can be specific for each network operator.

For definition of Group Call Reference (with leading zeros inserted as necessary) on the radio interface, A interface and Abis interface, see 3GPP TS 24.008 [5], 3GPP TS 44.068 [46] and 3GPP TS 44.069 [47].

For definition of Group Call Reference (also known as ASCI Call Reference, Voice Group Call Reference or Voice Broadcast Call Reference) coding on MAP protocol interfaces, see 3GPP TS 29.002 [31].

The format is given in figure 12.

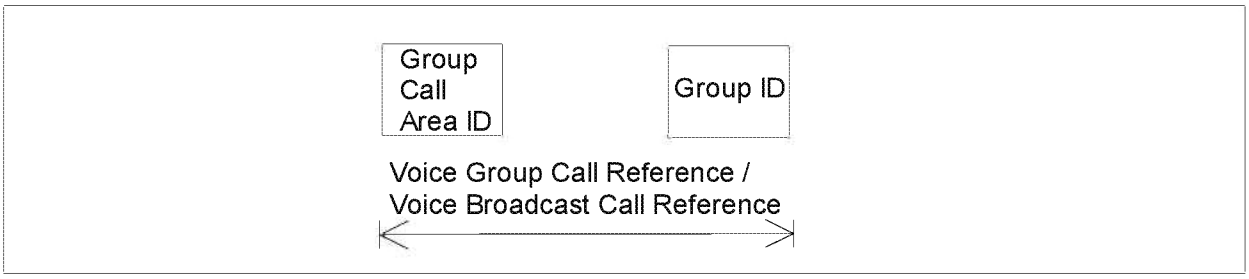

Figure 12: Voice Group Call Reference / Voice Broadcast Call Reference

8 SCCP subsystem numbers

Subsystem numbers are used to identify applications within network entities which use SCCP signalling. In GSM and UMTS, subsystem numbers may be used between PLMNs, in which case they are taken from the globally standardized range (1 - 31) or the part of the national network range (129 - 150) reserved for GSM/UMTS use between PLMNs. For use within a PLMN, they are taken from the part of the national network range (32 - 128 & 151 - 254) not reserved for GSM/UMTS use between PLMNs.

8.1 Globally standardized subsystem numbers used for GSM/UMTS

The following globally standardised subsystem numbers have been allocated for use by GSM/UMTS:

0000 0110HLR (MAP);

0000 0111VLR (MAP);

0000 1000MSC (MAP);

0000 1001EIR (MAP);

0000 1010is allocated for evolution (possible Authentication Centre).

8.2 National network subsystem numbers used for GSM/UMTS

The following national network subsystem numbers have been allocated for use within GSM/UMTS networks:

1111 1000CSS (MAP);

1111 1001PCAP;

1111 1010BSC (BSSAP-LE);

1111 1011MSC (BSSAP-LE);

1111 1100SMLC (BSSAP-LE);

1111 1101BSS O&M (A interface);

1111 1110BSSAP (A interface).

The following national network subsystem numbers have been allocated for use within and between GSM/UMTS networks:

1000 1110RANAP;

1000 1111RNSAP;

1001 0001GMLC (MAP);

1001 0010CAP;

1001 0011gsmSCF (MAP) or IM-SSF (MAP) or Presence Network Agent;

1001 0100SIWF (MAP);

1001 0101SGSN (MAP);

1001 0110GGSN (MAP).

9 Definition of Access Point Name

In the GPRS backbone, an Access Point Name (APN) is a reference to a GGSN. To support inter-PLMN roaming, the internal GPRS DNS functionality is used to translate the APN into the IP address of the GGSN.

9A Definition of Data Network Name

In 5GS, the Data Network Name (DNN) is equivalent to an APN in EPS. The DNN is a reference to a data network, it may be used e.g. to select SMF or UPF.

The requirements for APN in clause 9 shall apply for DNN in a 5GS as well.

9.0 General

Access Point Name as used in the Domain Name System (DNS) Procedures defined in 3GPP TS 29.303 [73] is specified in clause 19.4.2.2.

9.1 Structure of APN

The APN is composed of two parts as follows:

- The APN Network Identifier; this defines to which external network the GGSN/PGW is connected and optionally a requested service by the MS. This part of the APN is mandatory.
- The APN Operator Identifier; this defines in which PLMN GPRS/EPS backbone the GGSN/PGW is located. This part of the APN is optional.

NOTE 1: The APN Operator Identifier is mandatory on certain interfaces, see the relevant stage 3 specifications.

The APN Operator Identifier is placed after the APN Network Identifier. An APN consisting of both the Network Identifier and Operator Identifier corresponds to a DNS name of a GGSN/PGW; the APN has, after encoding as defined in the paragraph below, a maximum length of 100 octets.

The encoding of the APN shall follow the Name Syntax defined in RFC 2181 [18], RFC 1035 [19] and RFC 1123 [20]. The APN consists of one or more labels. Each label is coded as a one octet length field followed by that number of octets coded as 8 bit ASCII characters. Following RFC 1035 [19] the labels shall consist only of the alphabetic characters (A-Z and a-z), digits (0-9) and the hyphen (-). Following RFC 1123 [20], the label shall begin and end with either an alphabetic character or a digit. The case of alphabetic characters is not significant. The APN is not terminated by a length byte of zero.

NOTE 2: A length byte of zero is added by the SGSN/MME at the end of the APN before interrogating a DNS server.

For the purpose of presentation, an APN is usually displayed as a string in which the labels are separated by dots (e.g. "Label1.Label2.Label3").

9.1.1 Format of APN Network Identifier

The APN Network Identifier shall contain at least one label and shall have, after encoding as defined in clause 9.1 above, a maximum length of 63 octets. An APN Network Identifier shall not start with any of the strings "rac", "lac", "sgsn" or "rnc", and it shall not end in ".gprs", i.e. the last label of the APN Network Identifier shall not be "gprs". Further, it shall not take the value "*".

In order to guarantee uniqueness of APN Network Identifiers within or between GPRS/EPS PLMN, an APN Network Identifier containing more than one label shall correspond to an Internet domain name. This name should only be allocated by the PLMN if that PLMN belongs to an organisation which has officially reserved this name in the Internet domain. Other types of APN Network Identifiers are not guaranteed to be unique within or between GPRS/EPS PLMNs.

An APN Network Identifier may be used to access a service associated with a GGSN/PGW. This may be achieved by defining:

- an APN which corresponds to a FQDN of a GGSN/PGW, and which is locally interpreted by the GGSN/PGW as a request for a specific service, or
- an APN Network Identifier consisting of 3 or more labels and starting with a Reserved Service Label, or an APN Network Identifier consisting of a Reserved Service Label alone, which indicates a GGSN/PGW by the nature of the requested service. Reserved Service Labels and the corresponding services they stand for shall be agreed between operators who have GPRS/EPS roaming agreements.

9.1.2 Format of APN Operator Identifier

The APN Operator Identifier is composed of three labels. The last label (or domain) shall be "gprs". The first and second labels together shall uniquely identify the GPRS/EPS PLMN.

For each operator, there is a default APN Operator Identifier (i.e. domain name). This default APN Operator Identifier is derived from the IMSI as follows:

"mnc<MNC>.mcc<MCC>.gprs"

where:

"mnc" and "mcc" serve as invariable identifiers for the following digits.

<MNC> and <MCC> are derived from the components of the IMSI defined in clause 2.2.

This default APN Operator Identifier is used for home routed inter-PLMN roaming situations when attempting to translate an APN consisting only of a Network Identifier into the IP address of the GGSN/PGW in the HPLMN. The PLMN may provide DNS translations for other, more human-readable, APN Operator Identifiers in addition to the default Operator Identifier described above.

Alternatively, in the roaming case if the GGSN/PGW from the VPLMN is to be selected, the APN Operator Identifier for the UE is constructed from the serving network PLMN ID. In this case, the APN-OI replacement field, if received, shall be ignored.

In order to guarantee inter-PLMN DNS translation, the <MNC> and <MCC> coding used in the "mnc<MNC>.mcc<MCC>.gprs" format of the APN OI shall be:

- <MNC> = 3 digits
- <MCC> = 3 digits
- If there are only 2 significant digits in the MNC, one "0" digit is inserted at the left side to fill the 3 digits coding of MNC in the APN OI.

As an example, the APN OI for MCC 345 and MNC 12 will be coded in the DNS as "mnc012.mcc345.gprs".

The APN-OI replacement is only used for selecting the GGSN/PGW from the HPLMN. The format of the domain name used in the APN-OI replacement field (as defined in 3GPP TS 23.060 [3] and 3GPP TS 23.401 [72]) is the same as the default APN-OI as defined above except that it may be preceded by one or more labels each separated by a dot.

EXAMPLE 1: province1.mnc012.mcc345.gprs

EXAMPLE 2: ggsn-cluster-A.provinceB.mnc012.mcc345.gprs

The APN constructed using the APN-OI replacement field is only used for DNS translation. The APN when being sent to other network entities over GTP interfaces shall follow the rules as specified in 3GPP TS 23.060 [3] and 3GPP TS 23.401 [72].

9.2 Definition of the Wild Card APN

The APN field in the HLR may contain a wild card APN if the HPLMN operator allows the subscriber to access any network of a given PDP Type. If an SGSN has received such a wild card APN, it may either choose the APN Network Identifier received from the Mobile Station or a default APN Network Identifier for addressing the GGSN when activating a PDP context.

9.2.1 Coding of the Wild Card APN

The wild card APN is coded as an APN with "*" as its single label, (i.e. a length octet with value one, followed by the ASCII code for the asterisk).

9.3 Definition of Emergency APN

The Emergency APN (Em-APN) is an APN used to derive a PDN GW selected for IMS Emergency call support. The exact encoding of the Em-APN is the responsibility of each PLMN operator as it is only valid within a given PLMN.

10 Identification of the Cordless Telephony System entities

10.1 General description of CTS-MS and CTS-FP Identities

Every CTS-FP broadcasts a local identity - the Fixed Part Beacon Identity (FPBI) - which contains an Access Rights Identity. Every CTS-MS has both an Access Rights Key and a CTS Mobile Subscriber Identity (CTSMSI). These operate as a pair. A CTS-MS is allowed to access any CTS-FP which broadcasts an FPBI which can be identified by any of the CTS-MS Access Rights Keys of that CTS-MS. The CTS-MS Access Rights Key contains the FPBI and the FPBI Length Indicator (FLI) indicating the relevant part of the FPBI used to control access.

10.2 CTS Mobile Subscriber Identities

10.2.1 General

Each CTS-MS has one or more temporary identities which are used for paging and to request access. The structure and allocation principles of the CTS Mobile Subscriber Identities (CTSMSI) are defined below.

10.2.2 Composition of the CTSMSI

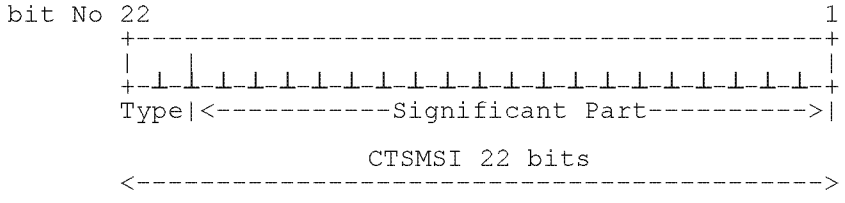

Figure 13: Structure of CTSMSI

The CTSMSI is composed of the following elements:

- CTSMSI Type. Its length is 2 bits;
- Significant Part. Its length is 20 bits.

The following CTSMSI Type values have been allocated for use by CTS:

00 Default Individual CTSMSI;

01 Reserved;

10 Assigned Individual CTSMSI;

11 Assigned Connectionless Group CTSMSI.

10.2.3 Allocation principles

The default Individual CTSMSI contains the least significant portion of the IMSI. This is the default CTS-MS identity.

Assigned CTSMSIs are allocated by the CTS-FP during enrolment, registration and other access procedures. Significant Part of the assigned CTSMSI shall be allocated in the range 00001-FFFFE. CTS-FP shall not allocate Significant Part equal to 00000 or to FFFFF and shall not allocate Assigned CTSMSI using Reserved Type value. Such assignments shall be ignored by the CTS-MS.

Assigned CTSMSIs are allocated in ciphered mode.

NOTE: The assigned individual CTSMSI should be updated whenever it is sent in clear text on the CTS radio interface during RR connection establishment.

The value FFFFF from the set of Assigned Connectionless Group CTSMSI shall be considered in all CTS-MS as the value of the Connectionless Broadcast Identifier.

10.2.4 CTSMSI hexadecimal representation

The 22 bits of CTSMSI are padded with 2 leading zeroes to give a 6 digit hexadecimal value.

EXAMPLE: binary CTSMSI value: 11 1001 0010 0000 1011 1100

hexadecimal CTSMSI value: 39 20 BC.

10.3 Fixed Part Beacon Identity

10.3.1 General

Each CTS-FP has one Fixed Part Beacon Identity known by the enrolled CTS-MSs. The FPBI is periodically broadcast on the BCH logical channel so that the CTS-MSs are able to recognise the identity of the CTS-FP. The FPBI contains an Access Rights Identity.

Enrolled CTS-MSs shall store the FPBI to which their assigned CTSMSIs are related.

Below the structure and allocation principles of the Fixed Part Beacon Identity (FPBI) are defined.

10.3.2 Composition of the FPBI

10.3.2.1 FPBI general structure

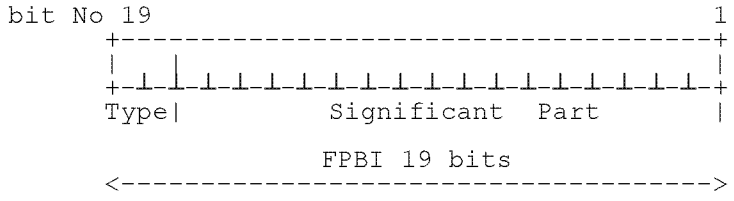

Figure 14: General structure of FPBI

The FPBI is composed of the following elements:

- FPBI Type. Its length is 2 bits;
- FPBI Significant Part. Its length is 17 bits.

NOTE: The three LSBs bits of the FPBI form the 3-bit training sequence code (TSC). See 3GPP TS 45.056 [35].

The following FPBI Type values have been allocated for use by CTS:

00 FPBI class A: residential and single-cell systems;

01 FPBI class B: multi-cell PABXs.

All other values are reserved and CTS-MSs shall treat these values as FPBI class A.

10.3.2.2 FPBI class A

This class is intended to be used for small residential and private (PBX) single cell CTS-FP.

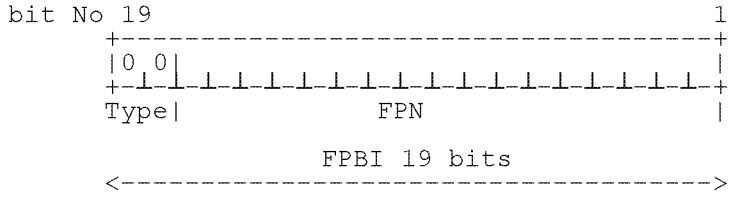

Figure 15: Structure of FPBI class A

The FPBI class A is composed of the following elements:

- FPBI Class A Type. Its length is 2 bits and its value is 00;
- Fixed Part Number (FPN). Its length is 17 bits. The FPN contains the least significant bits of the Serial Number part of the IFPEI.

The FPBI Length Indicator shall be set to 19 for a class A FPBI.

10.3.2.3 FPBI class B

This class is reserved for more complex private installation such as multi-cell PABXs.

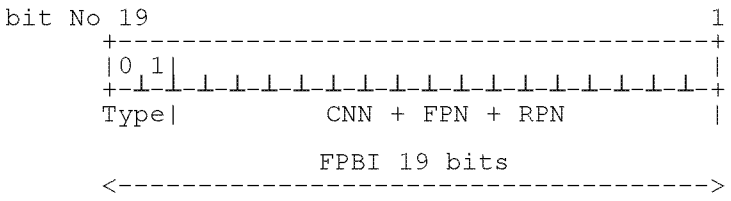

Figure 16: Structure of FPBI class B

The FPBI class B is composed of the following elements:

- FPBI Class B Type. Its length is 2 bits and its value is 01;
- CTS Network Number (CNN). Its length is defined by the manufacturer or the system installer;
- Fixed Part Number (FPN). Its length is defined by the manufacturer or the system installer;
- Radio Part Number (RPN) assigned by the CTS manufacturer or system installer. Its length is defined by the manufacturer or the system installer.

NOTE: RPN is used to separate a maximum of $2^{\text{RPN length}}$ different cells from each other. This defines a cluster of cells supporting intercell handover. RPN length is submitted to a CTS-MS as a result of a successful attachment.

The FPBI Length Indicator shall be set to (2 + CNN Length) for a class B FPBI.

10.3.3 Allocation principles

The FPBI shall be allocated during the CTS-FP initialisation procedure. Any change to the value of the FPBI of a given CTS-FP shall be considered as a CTS-FP re-initialisation; i.e. each enrolled CTS-MS needs to be enrolled again.

FPBI are not required to be unique (i.e. several CTS-FP can have the same FPBI in different areas). Care should be taken to limit CTS-MS registration attempts to a fixed part with the same FPBI as another fixed part.

10.4 International Fixed Part Equipment Identity

10.4.1 General

The structure and allocation principles of the International Fixed Part Equipment Identity (IFPEI) are defined below.

10.4.2 Composition of the IFPEI

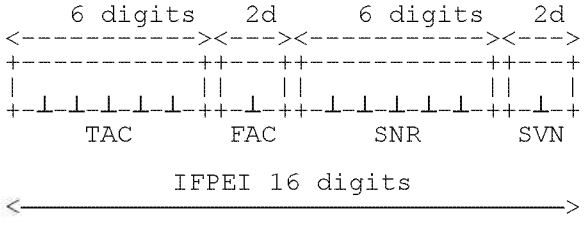

Figure 17: Structure of IFPEI

The IFPEI is composed of the following elements (each element shall consist of decimal digits only):

- Type Approval Code (TAC). Its length is 6 decimal digits;
- Final Assembly Code (FAC). Its length is 2 decimal digits;
- Serial NumbeR (SNR). Its length is 6 decimal digits;

- Software Version Number (SVN) identifies the software version number of the fixed part equipment. Its length is 2 digits.

Regarding updates of the IFPEI: the TAC, FAC and SNR shall be physically protected against unauthorised change (see 3GPP TS 42.009 [36]); i.e. only the SVN part of the IFPEI can be modified.

10.4.3 Allocation and assignment principles

The Type Approval Code (TAC) is issued by a global administrator.

The place of final assembly (FAC) is encoded by the manufacturer.

Manufacturers shall allocate unique serial numbers (SNR) in a sequential order.

The Software Version Number (SVN) is allocated by the manufacturer after authorisation by the type approval authority. SVN value 99 is reserved for future use.

10.5 International Fixed Part Subscription Identity

10.5.1 General

The structure and allocation principles of the International Fixed Part Subscription Identity (IFPSI) are defined below.

10.5.2 Composition of the IFPSI

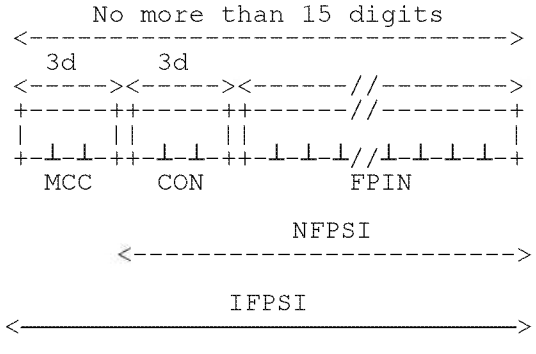

Figure 18: Structure of IFPSI

The IFPSI is composed of the following elements (each element shall consist of decimal digits only):

- Mobile Country Code (MCC) consisting of three digits. The MCC identifies the country of the CTS-FP subscriber (e.g. 208 for France);
- CTS Operator Number (CON). Its length is three digits;
- Fixed Part Identification Number (FPIN) identifying the CTS-FP subscriber.

The National Fixed Part Subscriber Identity (NFPSI) consists of the CTS Operator Number and the Fixed Part Identification Number.

10.5.3 Allocation and assignment principles

IFPSI shall consist of decimal characters (0 to 9) only.

The allocation of Mobile Country Codes (MCCs) is administered by the ITU.

The allocation of CTS Operator Number (CON) and the structure of National Fixed Part Subscriber Identity (NFPSI) may be responsibility of each national numbering plan administrator.

CTS Operators shall allocate unique Fixed Part Identification Numbers.

11 Identification of Localised Service Area

Cells may be grouped into specific localised service areas. Each localised service area is identified by a localised service area identity (LSA ID). No restrictions are placed on what cells may be grouped into a given localised service area.

The LSA ID can either be a PLMN significant number or a universal identity. This shall be known both in the networks and in the SIM.

The LSA ID consists of 24 bits, numbered from 0 to 23, with bit 0 being the LSB. Bit 0 indicates whether the LSA is a PLMN significant number or a universal LSA. If the bit is set to 0 the LSA is a PLMN significant number; if it is set to 1 it is a universal LSA.

The LSA ID shall be composed as shown in figure 19:

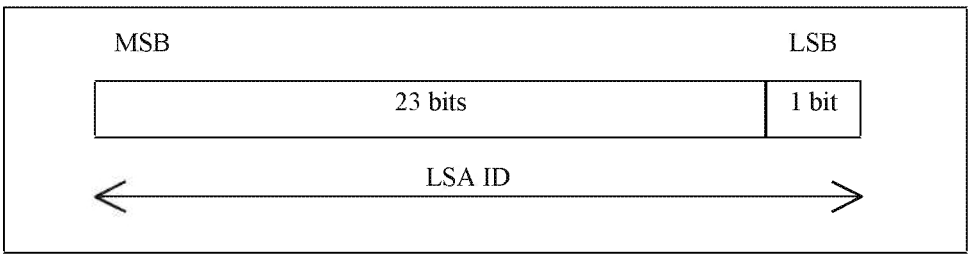

Figure 19: Structure of LSA ID

12 Identification of PLMN, RNC, Service Area, CN domain and Shared Network Area

The following clauses describe identifiers which are used by both the CN and the UTRAN across the Iu interface. For identifiers which are solely used within the UTRAN, see 3GPP TS 25.401 [16].

NOTE: in the following clauses, the double vertical bar notation || indicates the concatenation operator.

12.1 PLMN Identifier

A Public Land Mobile Network is uniquely identified by its PLMN identifier. PLMN-Id consists of Mobile Country Code (MCC) and Mobile Network Code (MNC).

- PLMN-Id = MCC || MNC

The MCC and MNC are predefined within a UTRAN, and set in the RNC via O&M.

12.2 CN Domain Identifier

A CN Domain Edge Node is identified within the UTRAN by its CN Domain Identifier. The CN Domain identifier is used over UTRAN interfaces to identify a particular CN Domain Edge Node for relocation purposes. The CN Domain identifier for Circuit Switching (CS) consists of the PLMN-Id and the LAC, whereas for Packet Switching (PS) it consists of the PLMN-Id, the LAC, and the RAC of the first accessed cell in the target RNS.

The two following CN Domain Identifiers are defined:

- CN CS Domain-Id = PLMN-Id || LAC
- CN PS Domain-Id = PLMN-Id || LAC || RAC

The LAC and RAC are defined by the operator, and set in the RNC via O&M.

For the syntax description and the use of this identifier in RANAP signalling, see 3GPP TS 25.413 [17].

12.3 CN Identifier

A CN node is uniquely identified within a PLMN by its CN Identifier (CN-Id). The CN-Id together with the PLMN identifier globally identifies the CN node. The CN-Id together with the PLMN-Id is used as the CN node identifier in RANAP signalling over the Iu interface.

- Global CN-Id = PLMN-Id || CN-Id

The CN-Id is defined by the operator, and set in the nodes via O&M.

For the syntax description and the use of this identifier in RANAP signalling, see 3GPP TS 25.413 [17].

12.4 RNC Identifier

An RNC node is uniquely identified by its RNC Identifier (RNC-Id). The RNC-Id of an RNC is used in the UTRAN, in a GERAN which is operating in GERAN Iu mode and between them. A BSC which is part of a GERAN operating in Iu mode is uniquely identified by its RNC Identifier (RNC-Id). The RNC-Id of a BSC is used in a GERAN which is operating in GERAN Iu mode, in the UTRAN and between them. RNC-Id together with the PLMN identifier globally identifies the RNC. The RNC-Id on its own or the RNC-Id together with the PLMN-Id is used as the RNC identifier in the UTRAN Iub, Iur and Iu interfaces. The SRNC-Id is the RNC-Id of the SRNC. The C-RNC-Id is the RNC-Id of the controlling RNC. The D-RNC-Id is the RNC Id of the drift RNC.

- Global RNC-Id = PLMN-Id || RNC-Id

The RNC-Id is defined by the operator, and set in the RNC via O&M

For the syntax description and the use of this identifier in RANAP signalling, see 3GPP TS 25.413 [17].

For the usage of this identifier on Iur-g, see 3GPP TS 43.130 [43].

12.5 Service Area Identifier

The Service Area Identifier (SAI) is used to identify an area consisting of one or more cells belonging to the same Location Area. Such an area is called a Service Area and can be used for indicating the location of a UE to the CN.

The Service Area Code (SAC) together with the PLMN-Id and the LAC constitute the Service Area Identifier.

- SAI = PLMN-Id || LAC || SAC

The SAC is defined by the operator, and set in the RNC via O&M.

For the syntax description and the use of this identifier in RANAP signalling, see 3GPP TS 25.413 [17].
3GPP TS 25.423 [37] and 3GPP TS 25.419 [38] define the use of this identifier in RNSAP and SABP signalling.

A cell may belong to one or two Service Areas. If it belongs to two Service Areas, one is applicable in the Broadcast (BC) domain and the other is applicable in both the CS and PS domains.

The Broadcast (BC) domain requires that its Service Areas each consist of only one cell. This does not limit the use of Service Areas for other domains. Refer to 3GPP TS 25.410 [39] for a definition of the BC domain.

12.6 Shared Network Area Identifier

The Shared Network Area Identifier (SNA-Id) is used to identify an area consisting of one or more Location Areas. Such an area is called a Shared Network Area and can be used to grant access rights to parts of a Shared Network to a UE in connected mode (see 3GPP TS 25.401 [39]).

The Shared Network Area Identifier consists of the PLMN-Id followed by the Shared Network Area Code (SNAC).

- SNA-Id = PLMN-Id || SNAC

The SNAC is defined by the operator.

For the syntax description and the use of this identifier in RANAP signalling, see 3GPP TS 25.413 [17].

12.7 Stand-Alone Non-Public Network Identifier

A Stand-Alone Non-Public Network (SNPN) is identified by a combination of PLMN-Identifier (see clause 12.1) and Network Identifier (NID) (see 3GPP TS 23.501 [119] clause 5.30.2).

The NID shall consist of an assignment model indication and an NID value as shown in figure 12.7-1.

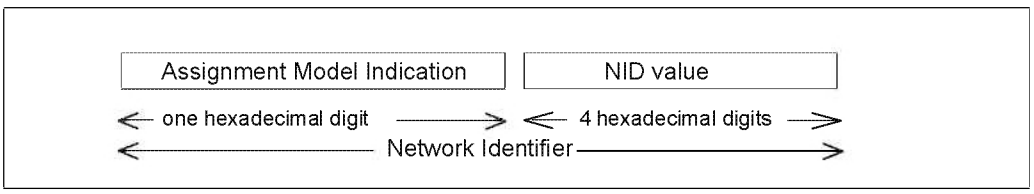

Figure 12.7-1: Network Identifier (NID)

Assignment Model 0 indicates: Universally managed NID.

Assignment Model 1 indicates: Locally managed NID.

Other Assignment Model values are reserved.

Editor's Note: FFS how to achieve that two different SNPN services providers do not use the same universally managed NID to identify their SNPNs.

Editor's Note: FFS whether 4 digits are sufficient for a NID value.

13 Numbering, addressing and identification within the IP multimedia core network subsystem

13.1 Introduction

This clause describes the format of the parameters needed to access the IP multimedia core network subsystem. For further information on the use of the parameters see 3GPP TS 23.228 [24] and 3GPP TS 29.163 [63]. For more information on the ".3gppnetwork.org" domain name and its applicability, see Annex D of the present document. For more information on the ".invalid" top level domain see IETF RFC 2606 [64].

13.2 Home network domain name

The home network domain name shall be in the form of an Internet domain name, e.g. operator.com, as specified in IETF RFC 1035 [19] and IETF RFC 1123 [20]. The home network domain name consists of one or more labels. Each label shall consist of the alphabetic characters (A-Z and a-z), digits (0-9) and the hyphen (-) in accordance with IETF RFC 1035 [19]. Each label shall begin and end with either an alphabetic character or a digit in accordance with IETF RFC 1123 [20]. The case of alphabetic characters is not significant.

For 3GPP systems, if there is no ISIM application, the UE shall derive the home network domain name from the IMSI as described in the following steps:

1. Take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used (see 3GPP TS 31.102 [27]) and separate them into MCC and MNC; if the MNC is 2 digits then a zero shall be added at the beginning.

2. Use the MCC and MNC derived in step 1 to create the "mnc<MNC>.mcc<MCC>.3gppnetwork.org" domain name.

3. Add the label "ims." to the beginning of the domain.

An example of a home network domain name is:

IMSI in use: 234150999999999;

where:

- MCC = 234;
- MNC = 15; and
- MSIN = 0999999999,

which gives the home network domain name: ims.mnc015.mcc234.3gppnetwork.org.

For 3GPP2 systems, if there is no IMC present, the UE shall derive the home network domain name as described in Annex C of 3GPP2 X.S0013-004 [67].

13.3 Private User Identity

The private user identity shall take the form of an NAI, and shall have the form username@realm as specified in clause 2.1 of IETF RFC 4282 [53].

NOTE: It is possible for a representation of the IMSI to be contained within the NAI for the private identity.

For 3GPP systems, the private user identity used for the user shall be as specified in clause 4.2 of 3GPP TS 24.229 [81] and in 3GPP TS 23.228 [24] Annex E.3.1. If the private user identity is not known, the private user identity shall be derived from the IMSI.

The following steps show how to build the private user identity out of the IMSI:

1. Use the whole string of digits as the username part of the private user identity; and

2. convert the leading digits of the IMSI, i.e. MNC and MCC, into a domain name, as described in clause 13.2.

The result will be a private user identity of the form "<IMSI>@ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org". For example: If the IMSI is 234150999999999 (MCC = 234, MNC = 15), the private user identity then takes the form "234150999999999@ims.mnc015.mcc234.3gppnetwork.org".

For 3GPP2 systems, if there is no IMC present, the UE shall derive the private user identity as described in Annex C of 3GPP2 X.S0013-004 [67].

13.4 Public User Identity

A Public User Identity is any identity used by a user within the IMS subsystem for requesting communication to another user.

The Public User Identity shall take the form of either a SIP URI (see IETF RFC 3261 [26]) or a Tel URI (see IETF RFC 3966 [45]).

The 3GPP specifications describing the interfaces over which Public User Identities are transferred specify the allowed Public User Identity formats, in particular 3GPP TS 24.229 [81] for SIP signalling interfaces, 3GPP TS 29.229 [95] for Cx and Dx interfaces, 3GPP TS 29.329 [96] for Sh interface, 3GPP TS 29.165 [97] for II-NNI interface.

In the case the user identity is a telephone number, it shall be represented either by a Tel URI or by a SIP URI that includes a "user=phone" URI parameter and a "userinfo" part that shall follow the same format as the Tel URI.

According to 3GPP TS 24.229 [81], the UE can use either:

- a global number as defined in IETF RFC 3966 [45] and following E.164 format, as defined by ITU-T Recommendation E.164 [10] or

- a local number, that shall include a "phone-context" parameter that identifies the scope of its validity, as per IETF RFC 3966 [45].

According to 3GPP TS 29.165 [97] a global number as defined in IETF RFC 3966 [45] shall be used in a tel-URI or in the user portion of a SIP URI with the user=phone parameter when conveyed via a non-roaming II-NNI except when agreement exists between the operators to also allow other kinds of numbers.

According to 3GPP TS 29.229 [95] and 3GPP TS 29.329 [96] the canonical forms of SIP URI and Tel URI shall be used over the corresponding Diameter interfaces.

The canonical form of a SIP URI for a Public User Identity shall take the form "sip:username@domain" as specified in IETF RFC 3261 [26], section 10.3. SIP URI comparisons shall be performed as defined in IETF RFC 3261 [26], section 19.1.4.

The canonical form of a Tel URI for a Public User Identity shall take the form "tel:+<CC><NDC><SN>" (max number of digits is 15), that represents an E.164 number and shall contain a global number without parameters and visual separators (see IETF RFC 3966[45], section 3). Tel URI comparisons shall be performed as defined in IETF RFC 3966[45], section 4.

Public User Identities are stored in the HSS either as a distinct Public User Identity or as a Wildcarded Public User Identity. A distinct Public User Identity contains the Public User Identity that is used in routing and it is explicitly provisioned in the HSS.

13.4A Wildcarded Public User Identity

Public User Identities may be stored in the HSS as Wildcarded Public User Identities. A Wildcarded Public User Identity represents a collection of Public User Identities that share the same service profile and are included in the same implicit registration set. Wildcarded Public User Identities enable optimisation of the operation and maintenance of the nodes for the case in which a large amount of users are registered together and handled in the same way by the network. The format of a Wildcarded Public User Identity is the same as for the Wildcarded PSI described in clause 13.5.

13.4B Temporary Public User Identity

For 3GPP systems, if there is no ISIM application to host the Public User Identity, a Temporary Public User Identity shall be derived, based on the IMSI. The Temporary Public User Identity shall be of the form as described in clause 13.4 and shall consist of the string "sip:" appended with a username and domain portion equal to the IMSI derived Private User Identity, as described in clause 13.2. An example using the same example IMSI from clause 13.2 can be found below:

EXAMPLE: "sip:234150999999999@ims.mnc015.mcc234.3gppnetwork.org".

For 3GPP2 systems, if there is no IMC present, the UE shall derive the public user identity as described in Annex C of 3GPP2 X.S0013-004 [67].

13.5 Public Service Identity (PSI)

The public service identity shall take the form of either a SIP URI (see IETF RFC 3261 [26]) or a Tel URI (see IETF RFC 3966 [45]). A public service identity identifies a service, or a specific resource created for a service on an application server. The domain part is pre-defined by the IMS operators and the IMS system provides the flexibility to dynamically create the user part of the PSIs.

The PSIs are stored in the HSS either as a distinct PSI or as a wildcarded PSI. A distinct PSI contains the PSI that is used in routing , whilst a wildcarded PSI represents a collection of PSIs. Wildcarded PSIs enable optimisation of the operation and maintenance of the nodes. A wildcarded PSI consists of a delimited regular expression located either in the userinfo portion of the SIP URI or in the telephone-subscriber portion of the Tel URI. The regular expression in the wildcarded PSI shall take the form of Extended Regular Expressions (ERE) as defined in chapter 9 in IEEE 1003.1-2004 Part 1 [60]. The delimiter shall be the exclamation mark character ("!"). If more than two exclamation mark characters are present in the userinfo portion or telephone-subscriber portion of a wildcarded PSI then the outside pair

of exclamation mark characters is regarded as the pair of delimiters (i.e. no exclamation mark characters are allowed to be present in the fixed parts of the userinfo portion or telephone-subscriber portion).

When stored in the HSS, the wildcarded PSI shall include the delimiter character to indicate the extent of the part of the PSI that is wildcarded. It is used to separate the regular expression from the fixed part of the wildcarded PSI.

Example: The following PSI could be stored in the HSS - "sip:chatlist!.*!@example.com".

When used on an interface, the exclamation mark characters within a PSI shall not be interpreted as delimiter..

Example: The following PSIs communicated in interface messages to the HSS will match to the wildcarded PSI of "sip:chatlist!.*!@example.com" stored in the HSS:

sip:chatlist1@example.com

sip:chatlist2@example.com

sip:chatlist42@example.com

sip:chatlistAbC@example.com

sip:chatlist!1@example.com

Note that sip:chatlist1@example.com and sip:chatlist!1@example.com are regarded different specific PSIs, both matching the wildcarded PSI sip:chatlist!.*!@example.com.

When used by an application server to identify a specific resource (e.g. a chat session) over Inter Operator Network to Network Interface (II-NNI), the PSI should be a SIP URI without including a port number.

NOTE: Based on local configuration policy, a PSI can be routed over Inter Operator Network to Network Interface (II-NNI). Details of this routing are operator specific and out of scope of this specification.

13.5A Private Service Identity

The Private Service Identity is applicable to a PSI user and is similar to a Private User Identity in the form of a Network Access Identifier (NAI), which is defined in IETF RFC 4282 [53]. The Private Service Identity is operator defined and although not operationally used for registration, authorisation and authentication in the same way as Private User Identity, it enables Public Service Identities to be associated to a Private Service Identity which is required for compatibility with the Cx procedures.

13.6 Anonymous User Identity

The Anonymous User Identity shall take the form of a SIP URI (see IETF RFC 3261 [26]). A SIP URI for an Anonymous User Identity shall take the form "sip:user@domain". The user part shall be the string "anonymous" and the domain part shall be the string "anonymous.invalid". The full SIP URI for Anonymous User Identity is thus:

"sip:anonymous@anonymous.invalid"

For more information on the Anonymous User Identity and when it is used, see 3GPP TS 29.163 [63].

13.7 Unavailable User Identity

The Unavailable User Identity shall take the form of a SIP URI (see IETF RFC 3261 [26]). A SIP URI for an Unavailable User Identity shall take the form "sip:user@domain". The user part shall be the string "unavailable" and the domain part shall be the string "unknown.invalid". The full SIP URI for Unavailable User Identity is thus:

"sip:unavailable@unknown.invalid"

For more information on the Unavailable User Identity and when it is used, see 3GPP TS 29.163 [63].

13.8 Instance-ID

An instance-id is a SIP Contact header parameter that uniquely identifies the SIP UA performing a registration.

When an IMEI is available, the instance-id shall take the form of a IMEI URN (see RFC 7254 [79]). The format of the instance-id shall take the form "urn:gsma:imei:<imeival>" where by the imeival shall contain the IMEI encoded as defined in RFC 7254 [79]. The optional <sw-version-param> and <imei-version-param> parameters shall not be included in the instance-id. RFC 7255 [104] specifies additional considerations for using the IMEI as an instance-id. An example of such an instance-id is as follows:

EXAMPLE: urn:gsma:imei:90420156-025763-0

If no IMEI is available, the instance-id shall take the form of a string representation of a UUID as a URN as defined in IETF RFC 4122 [80]. An example of such an instance-id is as follows:

EXAMPLE: urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6

For more information on the instance-id and when it is used, see 3GPP TS 24.229 [81].

13.9 XCAP Root URI

13.9.1 XCAP Root URI on Ut interface

13.9.1.1 General

XCAP Root URI is an HTTP URI that represents the XCAP Root. Although a valid URI, the XCAP Root URI does not correspond to an actual resource.

13.9.1.2 Format of XCAP Root URI

The XCAP Root URI, as defined in IETF RFC 4825 [94], is an HTTP URI that should have the following format:

"http://xcap.<domain>"

in which "<domain>" identifies the domain hosting the XCAP server.

NOTE 1: The XCAP Root URI does not contain a port portion or an abs path portion of a standard HTTP URI.

If a preconfigured or provisioned XCAP Root URI is available then the UE shall use it. When a preconfigured or provisioned XCAP Root URI does not exist then the UE shall create the XCAP Root URI as follows:

- The first label shall be "xcap".
- The next label(s) shall identify the home network as follows:
  1. When the UE has an ISIM, the domain name from the IMPI shall be used (see 3GPP TS 31.103 [93]) as follows:
     a. if the last two labels of the domain name from the IMPI are "3gppnetwork.org":
        i. the next labels shall be all labels of the domain name from the IMPI apart from the last two labels; and
        ii. the last three labels shall be "pub.3gppnetwork.org";
     b. if the last two labels of the domain name from the IMPI are other than the "3gppnetwork.org":
        i. the next labels shall be all labels of the domain name from the IMPI;
  2. When the UE has a USIM and does not have ISIM, the home network shall be "ims.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org" where <MNC> and <MCC> shall be derived from the components of the IMSI defined in clause 2.2. If there are only two significant digits in the MNC, one "0" digit shall be inserted at the left side to fill the 3 digits coding of MNC in the FQDN of XCAP Root URI.

As an example for the case when the UE has ISIM, where the IMPI is "user@operator.com", the overall XCAP Root URI used by the UE would be:

"http://xcap.operator.com".

As an example for the case when the UE has ISIM, where the IMPI is "234150999999999@ims.mnc015.mcc234.3gppnetwork.org", the overall XCAP Root URI used by the UE would be:

"xcap.ims.mnc015.mcc234.pub.3gppnetwork.org".

As an example for the case when the UE has USIM and does not have ISIM, where the MCC is 345 and the MNC is 12, the overall XCAP Root URI created and used by the UE would be:

"xcap.ims.mnc012.mcc345.pub.3gppnetwork.org"

13.10 Default Conference Factory URI for MMTel

The Default Conference Factory URI for MMTel shall take the form of a SIP URI (see IETF RFC 3261 [26]) with a host portion set to the home network domain name as described in clause 13.2 prefixed with "conf-factory.". The user portion shall be set to "mmtel".

Examples of the Default Conference Factory URI for MMTel can be found below:

EXAMPLE 1: "sip:mmtel@conf-factory.operator.com"

when the UE has a home network domain name of operator.com.

EXAMPLE 2: "sip:mmtel@conf-factory.ims.mnc015.mcc234.3gppnetwork.org"

for 3GPP systems, when the UE with no ISIM application has a home network domain name of ims.mnc015.mcc234.3gppnetwork.org derived from the same example IMSI as described in clause 13.2.

13.11 Unknown User Identity

The Unknown User Identity shall take the form of a SIP URI (see IETF RFC 3261 [26]). A SIP URI for an Unknown User Identity shall take the form "sip:user@domain". The user part shall be the string "unknown" and the domain part shall be the string "unknown.invalid". The full SIP URI for Unknown User Identity is thus:

"sip:unknown@unknown.invalid"

For more information on the Unknown User Identity and when it is used, see 3GPP TS 29.163 [63], clauses 7.4.6 and 7.5.4.

13.12 Default WWSF URI

13.12.1 General

Default WWSF URI is an HTTP URI that represents the WebRTC Web Server Function (WWSF) defined in 3GPP TS 23.228 [24].

13.12.2 Format of the Default WWSF URI

The Default WWSF URI is an HTTP URI that should have the following format:

"http://wwsf.<domain>"

in which "<domain>" identifies the domain hosting the WWSF.

If a preconfigured or provisioned WWSF URI is available then the UE shall use it. When a preconfigured or provisioned WWSF URI does not exist then the UE shall create the Default WWSF URI as follows:

- The first label shall be "wwsf".
- The next label(s) shall identify the home network as follows:

1. When the UE has an ISIM, the domain name from the IMPI shall be used (see 3GPP TS 31.103 [93]) as follows:

   a. if the last two labels of the domain name from the IMPI are "3gppnetwork.org":

      i. the next labels shall be all labels of the domain name from the IMPI apart from the last two labels; and

      ii. the last three labels shall be "pub.3gppnetwork.org";

   b. if the last two labels of the domain name from the IMPI are other than the "3gppnetwork.org":

      i. the next labels shall be all labels of the domain name from the IMPI;

2. When the UE has a USIM and does not have an ISIM, the home network shall be "ims.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org" where <MNC> and <MCC> shall be derived from the components of the IMSI defined in clause 2.2. If there are only two significant digits in the MNC, one "0" digit shall be inserted at the left side to fill the 3 digits coding of MNC in the FQDN of WWSF URI.

As an example for the case when the UE has the ISIM, where the IMPI is "user@operator.com", the Default WWSF URI used by the UE would be:

EXAMPLE 1: "http://wwsf.operator.com".

As an example for the case when the UE has the ISIM, where the IMPI is "234150999999999@ims.mnc015.mcc234.3gppnetwork.org", the Default WWSF URI used by the UE would be:

EXAMPLE 2: "http://wwsf.ims.mnc015.mcc234.pub.3gppnetwork.org".

As an example for the case when the UE has the USIM and does not have the ISIM, where the MCC is 345 and the MNC is 12, the Default WWSF URI created and used by the UE would be:

EXAMPLE 3: "http://wwsf.ims.mnc012.mcc345.pub.3gppnetwork.org".

13.13 IMEI based identity

The IMEI based identity shall take the form of a SIP URI (see IETF RFC 3261 [26]). The IMEI based identity is included in P-Preferred-Identity header field of SIP INVITE request by the UE and used in cases of unauthenticated emergency sessions as specified in clause 5.1.6.8.2 of 3GPP TS 24.229 [81]. A SIP URI for an IMEI based identity shall take the form "sip:user@domain" where by the user part shall contain the IMEI. The IMEI shall be encoded according to ABNF of imeival as defined in IETF RFC 7254 [79]. The domain part shall contain the home network domain named derived as specified in clause 13.2.

An example for the case when the UE has a home network domain name of operator.com is:

EXAMPLE 1: "sip:90420156-025763-0@operator.com"

An example for 3GPP systems, when the UE with no ISIM application has a home network domain name of ims.mnc015.mcc234.3gppnetwork.org derived from the same example IMSI from clause 13.2 is:

EXAMPLE 2: "sip:90420156-025763-0@ims.mnc015.mcc234.3gppnetwork.org"

14 Numbering, addressing and identification for 3GPP System to WLAN Interworking

14.1 Introduction

This clause describes the format of the parameters needed to access the 3GPP system supporting the WLAN interworking. For further information on the use of the parameters see 3GPP TS 24.234 [48]. For more information on the ".3gppnetwork.org" domain name and its applicability, see Annex D of the present document.

NOTE: The WLAN Network Selection and WLAN/3GPP Radio Interworking features supersede the I-WLAN feature from Rel-12 onwards, therefore all I-WLAN related requirements specified in the present Clause are no longer maintained.

14.2 Home network realm

The home network realm shall be in the form of an Internet domain name, e.g. operator.com, as specified in RFC 1035 [19].

When attempting to authenticate within WLAN access, the WLAN UE shall derive the home network domain name from the IMSI as described in the following steps:

1. take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used (see 3GPP TS 31.102 [27], 3GPP TS 51.011 [66]) and separate them into MCC and MNC; if the MNC is 2 digits then a zero shall be added at the beginning;
2. use the MCC and MNC derived in step 1 to create the "mnc<MNC>.mcc<MCC>. 3gppnetwork.org" domain name;
3. add the label "wlan." to the beginning of the domain name.

An example of a WLAN NAI realm is:

IMSI in use: 234150999999999;

Where:

MCC = 234;

MNC = 15;

MSIN = 0999999999

Which gives the home network domain name: wlan.mnc015.mcc234.3gppnetwork.org.

NOTE: If it is not possible for the WLAN UE to identify whether a 2 or 3 digit MNC is used (e.g. SIM is inserted and the length of MNC in the IMSI is not available in the "Administrative data" data file), it is implementation dependent how the WLAN UE determines the length of the MNC (2 or 3 digits).

14.3 Root NAI

The Root NAI shall take the form of a NAI, and shall have the form username@realm as specified in clause 2.1 of IETF RFC 4282 [53].

The username part format of the Root NAI shall comply with IETF RFC 4187 [50] when EAP AKA authentication is used and with IETF RFC 4186 [51], when EAP SIM authentication is used.

When the username part includes the IMSI, the Root NAI shall be built according to the following steps:

1. Generate an identity conforming to NAI format from IMSI as defined in EAP SIM [51] and EAP AKA [50] as appropriate;
2. Convert the leading digits of the IMSI, i.e. MNC and MCC, into a domain name, as described in clause 14.2.

The result will be a root NAI of the form:

"0<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org", for EAP AKA authentication and
"1<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org", for EAP SIM authentication

For example, for EAP AKA authentication: If the IMSI is 234150999999999 (MCC = 234, MNC = 15), the root NAI then takes the form 0234150999999999@wlan.mnc015.mcc234.3gppnetwork.org.

14.4 Decorated NAI

The Decorated NAI shall take the form of a NAI and shall have the form 'homerealm!username@otherrealm' as specified in clause 2.7 of the IETF RFC 4282 [53].

The realm part of Decorated NAI consists of 'otherrealm', see the IETF draft 2486-bisRFC 4282 [53]. 'Homerealm' is the realm as specified in clause 14.2, using the HPLMN ID ('homeMCC' + 'homeMNC)'. 'Otherrealm' is the realm built using the PLMN ID (visitedMCC + visited MNC) of the PLMN selected as a result of WLAN PLMN selection (see 3GPP TS 24.234 [48]).

The username part format of the Root NAI shall comply with IETF RFC 4187 [50] when EAP AKA authentication is used and with IETF RFC 4186 [51], when EAP SIM authentication is used.

When the username part of Decorated NAI includes the IMSI, it shall be built following the same steps specified for Root NAI in clause 14.3.

The result will be a decorated NAI of the form:

"wlan.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org
!0<IMSI>@wlan.mnc<visitedMNC>.mcc<visitedMCC>.3gppnetwork.org", for EAP AKA authentication and "
wlan.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org
!1<IMSI>@wlan.mnc<visitedMNC>.mcc<visitedMCC>.3gppnetwork.org ", for EAP SIM authentication

For example, for EAP AKA authentication: If the IMSI is 234150999999999 (MCC = 234, MNC = 15) and the PLMN ID of the Selected PLMN is MCC = 610, MNC = 71 then the Decorated NAI takes the form wlan.mnc015.mcc234.3gppnetwork.org!0234150999999999@wlan.mnc071.mcc610.3gppnetwork.org.

NOTE: the 'otherrealm' specified in the present document is resolved by the WLAN AN. If the WLAN AN does not have access to the GRX, then the WLAN AN should resolve the realm by other means e.g. static look-up table, private local DNS server acting as an authoritative name server for that sub-domain.

14.4A Fast Re-authentication NAI

The Fast Re-authentication NAI in both EAP-SIM and EAP-AKA shall take the form of a NAI as specified in clause 2.1 of IETF RFC 4282 [53]. If the 3GPP AAA server does not return a complete NAI, the Fast Re-authentication NAI shall consist of the username part of the fast re-authentication identity as returned from the 3GPP AAA server and the same realm as used in the permanent user identity. If the 3GPP AAA server returns a complete NAI as the re-authentication identity, then this NAI shall be used. The username part of the fast re-authentication identity shall be decorated as described in 14.4 if the Selected PLMN is different from the HPLMN.

NOTE: The permanent user identity is either the root or decorated NAI as defined in clauses 14.3 and 14.4.

EXAMPLE 1: If the fast re-authentication identity returned by the 3GPP AAA Server is 458405627015 and the IMSI is 234150999999999 (MCC = 234, MNC = 15), the Fast Re-authentication NAI for the case when NAI decoration is not used takes the form: 458405627015@wlan.mnc015.mcc234.3gppnetwork.org

EXAMPLE 2: If the fast re-authentication identity returned by the 3GPP AAA Server is "458405627015@aaa1.wlan.mnc015.mcc234.3gppnetwork.org" and the IMSI is 234150999999999 (MCC = 234, MNC = 15), the Fast Re-authentication NAI for the case when NAI decoration is not used takes the form: 458405627015@aaa1.wlan.mnc015.mcc234.3gppnetwork.org

EXAMPLE 3: If the fast re-authentication identity returned by the 3GPP AAA Server is 458405627015 and the IMSI is 234150999999999 (MCC = 234, MNC = 15), and the PLMN ID of the Selected PLMN is MCC = 610, MNC = 71, the Fast Re-authentication NAI takes the form:
wlan.mnc015.mcc234.3gppnetwork.org !458405627015@wlan.mnc071.mcc610.3gppnetwork.org

14.5 Temporary identities

The Temporary identities (Pseudonyms and re-authentication identities) shall take the form of a NAI username as specified in clause 2.1 of the IETF RFC 4282 [53].

Temporary identity shall be generated as specified in clause 6.4.1 of 3GPP TS 33.234 [55]. This part of the temporary identity shall follow the UTF-8 transformation format specified in IETF RFC 2279 [54] except for the following reserved hexadecimal octet value:

FF.

When the temporary identity username is coded with FF, this reserved value is used to indicate the special case when no valid temporary identity exists in the WLAN UE (see 3GPP TS 24.234 [48]). The network shall not allocate a temporary identity with the whole username coded with the reserved hexadecimal value FF.

For EAP-AKA authentication, the username portion of the pseudonym identity shall be prepended with the single digit "2" and the username portion of the fast re-authentication identity shall be prepended with the single digit "4" as specified in clause 4.1.1.7 of IETF RFC 4187 [50].

For EAP-SIM authentication, the username portion of the pseudonym identity shall be prepended with the single digit "3" and the username portion of the fast re-authentication identity shall be prepended with the single digit "5" as specified in clause 4.2.1.7 of IETF RFC 4186 [51].

14.6 Alternative NAI

The Alternative NAI shall take the form of a NAI, i.e. 'any_username@REALM' as specified of IETF RFC 4282 [53]. The Alternative NAI shall not be routable from any AAA server.

The Alternative NAI shall contain a username part which is not derived from the IMSI. The username part shall not be a null string.

The REALM part of the NAI shall be "unreachable.3gppnetwork.org".

The result shall be an NAI in the form of:

"<any_non_null_string>@unreachable.3gppnetwork.org"

14.7 W-APN

The W-APN is composed of two parts as follows:

- The W-APN Network Identifier; this defines to which external network the PDG is connected.
- The W-APN Operator Identifier; this defines in which PLMN the PDG serving the W-APN is located.

The W-APN Operator Identifier is placed after the W-APN Network Identifier. The W-APN consisting of both the Network Identifier and Operator Identifier corresponds to a FQDN of a PDG; the W-APN has, after encoding as defined in the paragraph below, a maximum length of 100 octets.

The encoding of the W-APN shall follow the Name Syntax defined in IETF RFC 2181 [18], IETF RFC 1035 [19] and IETF RFC 1123 [20]. The W-APN consists of one or more labels. Each label is coded as a one octet length field followed by that number of octets coded as 8 bit ASCII characters. Following IETF RFC 1035 [19] the labels shall consist only of the alphabetic characters (A-Z and a-z), digits (0-9) and the hyphen (-). Following IETF RFC 1123 [20], the label shall begin and end with either an alphabetic character or a digit. The case of alphabetic characters is not significant. The W-APN is not terminated by a length byte of zero.

For the purpose of presentation, a W-APN is usually displayed as a string in which the labels are separated by dots (e.g. "Label1.Label2.Label3").

The W-APN for the support of IMS Emergency calls shall take the form of a common, reserved Network Identifier described in clause 14.7.1 together with the usual W-APN Operator Identifier as described in clause 14.7.2.

14.7.1 Format of W-APN Network Identifier

The W-APN Network Identifier follows the format defined for APNs in clause 9.1.1. In addition to what has been defined in clause 9.1.1 the W-APN Network Identifier shall not contain "w-apn." and not end in ".3gppnetwork.org".

A W-APN Network Identifier may be used to access a service associated with a PDG. This may be achieved by defining:

- a W-APN which corresponds to a FQDN of a PDG, and which is locally interpreted by the PDG as a request for a specific service, or
- a W-APN Network Identifier consisting of 3 or more labels and starting with a Reserved Service Label, or a W-APN Network Identifier consisting of a Reserved Service Label alone, which indicates a PDG by the nature of the requested service. Reserved Service Labels and the corresponding services they stand for shall be agreed between operators who have WLAN roaming agreements.

The W-APN Network Identifier for the support of IMS Emergency calls shall take the form of a common, reserved Network Identifier of the form "sos".

As an example, the W-APN for MCC 345 and MNC 12 is coded in the DNS as:

"sos.w-apn.mnc012.mcc345.pub.3gppnetwork.org".

where "sos" is the W-APN Network Identifier and " mnc012.mcc345.pub.3gppnetwork.org " is the W-APN Operator Identifier.

14.7.2 Format of W-APN Operator Identifier

The W-APN Operator Identifier is composed of six labels. The last three labels shall be "pub.3gppnetwork.org". The second and third labels together shall uniquely identify the PLMN. The first label distinguishes the domain name as a W-APN.

For each operator, there is a default W-APN Operator Identifier (i.e. domain name). This default W-APN Operator Identifier is derived from the IMSI as follows:

"w-apn.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org"

where:

"mnc" and "mcc" serve as invariable identifiers for the following digits.

<MNC> and <MCC> are derived from the components of the IMSI defined in clause 2.2.

Alternatively, the default W-APN Operator Identifier is derived using the MNC and MCC of the VPLMN. See 3GPP TS 24.234 [48] for more information.

The default W-APN Operator Identifier is used in both non-roaming and roaming situations when attempting to translate a W-APN consisting only of a Network Identifier into the IP address of the PDG in the HPLMN.

In order to guarantee inter-PLMN DNS translation, the <MNC> and <MCC> coding used in the "w-apn.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org" format of the W-APN OI shall be:

- <MNC> = 3 digits
- <MCC> = 3 digits

If there are only 2 significant digits in the MNC, one "0" digit shall be inserted at the left side to fill the 3 digits coding of MNC in the W-APN OI.

As an example, the W-APN OI for MCC 345 and MNC 12 is coded in the DNS as:

"w-apn.mnc012.mcc345.pub.3gppnetwork.org".

14.7.3 Alternative Format of W-APN Operator Identifier

For situations when the PDG serving the W-APN is located in such network that is not part of the GRX (i.e. the Interoperator IP backbone), the default Operator Identifier described in clause 14.7.2 is not available for use. This restriction originates from the ".3gppnetwork.org" domain, which is only available in GRX DNS for actual use. Thus an alternative format of W-APN Operator Identifier is required for this case.

The Alternative W-APN Operator Identifiers shall be constructed as follows:

"w-apn.<valid operator's REALM>"

where:

<valid operator's REALM> corresponds to REALM names owned by the operator hosting the PDG serving the desired W-APN.

REALM names are required to be unique, and are piggybacked on the administration of the Public Internet DNS namespace. REALM names may also belong to the operator of the VPLMN.

As an example, the W-APN OI for the Operator REALM "notareal.com" is coded in the Public Internet DNS as:

"w-apn.notareal.com".

14.8 Emergency Realm and Emergency NAI for Emergency Cases

The emergency realm shall be of the form of a home network realm as described in clause 14.2 prefixed with the label "sos." at the beginning of the domain name.

An example of a WLAN emergency NAI realm is:

IMSI in use: 234150999999999;

Where:

MCC = 234;

MNC = 15;

MSIN = 0999999999

Which gives the home network domain name: sos.wlan.mnc015.mcc234.3gppnetwork.org.

The NAI for emergency cases shall be of the form as specified in clauses 14.3 and 14.4, with the addition of the emergency realm as described above for PLMNs where the emergency realm is supported.

When UE is using I-WLAN as the access network for IMS emergency calls and IMSI is not available, the Emergency NAI shall be an NAI compliant with IETF RFC 4282 [53] consisting of username and realm, either constructed with IMEI or MAC address, as specified in 3GPP TS 33.234 [55]. The exact format shall be:

imei<IMEI>@sos.wlan.mnc<visitedMNC>.mcc<visitedMCC>.3gppnetwork.org

or if IMEI is not available,

mac<MAC>@sos.wlan.mnc<visitedMNC>.mcc<visitedMCC>.3gppnetwork.org

The realm part of the above NAI consists of the realm built using the PLMN ID (visitedMCC + visitedMNC) of the PLMN selected as a result of the network selection procedure, as specified in clause 5.2.5.4 of the 3GPP TS 24.234 [48].

The MNC and MCC shall be with 3 digits coded. If there are only 2 significant digits in the MNC, one "0" digit shall be inserted at the left side to fill the 3 digits coding of MNC in the realm of the NAI.

For example, if the IMEI is 219551288888888, and the selected PLMN is with MCC 345 and MNC 12, the Emergency NAI then takes the form of imei219551288888888@sos.wlan.mnc012.mcc345.3gppnetwork.org.

For example, if the MAC address is 44-45-53-54-00-AB, and the selected PLMN is with MCC 345 and MNC 12, the Emergency NAI then takes the form of mac4445535400AB@sos.wlan.mnc012.mcc345.3gppnetwork.org, where the MAC address is represented in hexadecimal format without separators.

15 Identification of Multimedia Broadcast/Multicast Service

15.1 Introduction

This clause describes the format of the parameters needed to access the Multimedia Broadcast/Multicast service. For further information on the use of the parameters see 3GPP TS 23.246 [52].

15.2 Structure of TMGI

Temporary Mobile Group Identity (TMGI) is used within MBMS to uniquely identify Multicast and Broadcast bearer services.

TMGI is composed as shown in figure 15.2.1.

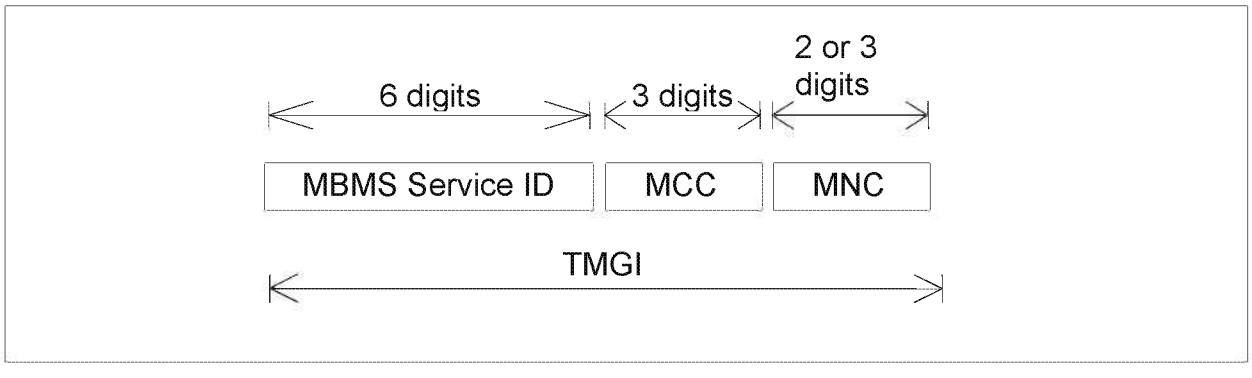

Figure 15.2.1: Structure of TMGI

The TMGI is composed of three parts:

1) MBMS Service ID consisting of three octets. MBMS Service ID consists of a 6-digit fixed-length hexadecimal number between 000000 and FFFFFF. MBMS Service ID uniquely identifies an MBMS bearer service within a PLMN. The structure of MBMS Service ID for services for Receive only mode is defined in 3GPP TS 24.116 [118].

2) Mobile Country Code (MCC) consisting of three digits. The MCC identifies uniquely the country of domicile of the BM-SC, except for the MCC value of 901, which does not identify any country and is assigned globally by ITU;

3) Mobile Network Code (MNC) consisting of two or three digits (depending on the assignment to the PLMN by its national numbering plan administrator). The MNC identifies the PLMN which the BM-SC belongs to, except for the MNC value of 56 when the MCC value is 901, which does not identify any PLMN. For more information on the use of the TMGI, see 3GPP TS 23.246 [52].

Any TMGI with MCC=901 and MNC=56 is used only for services for Receive Only Mode (see TS 23.246 [52] and 3GPP TS 24.116 [118]).

15.3 Structure of MBMS SAI

The MBMS Service Area (MBMS SA) is defined in 3GPP TS 23.246 [52]. It comprises of one or more MBMS Service Area Identities (MBMS SAIs), in any case each MBMS SA shall not include more than 256 MBMS SAIs. An MBMS

SAI shall identify a group of cells within a PLMN, that is independent of the associated Location/Routing/Service Area and the physical location of the cell(s). A cell shall be able to belong to one or more MBMS SAs, and therefore is addressable by one or more MBMS SAIs.

The MBMS SAI shall be a decimal number between 0 and 65,535 (inclusive). The value 0 has a special meaning; it shall denote the whole PLMN as the MBMS Service Area and it shall indicate to a receiving RNC/BSS/MCE that all cells reachable by that RNC/BSS/MCE shall be part of the MBMS Service Area.

With the exception of the specific MBMS Service Area Identity with value 0, the MBMS Service Area Identity shall be unique within a PLMN and shall be defined in such a way that all the corresponding cells are MBMS capable.

15.4 Home Network Realm

The home network realm shall be in the form of an Internet domain name, e.g. operator.com, as specified in IETF RFC 1035 [19] and IETF RFC 1123 [20]. The home network realm consists of one or more labels. Each label shall consist of the alphabetic characters (A-Z and a-z), digits (0-9) and the hyphen (-) in accordance with IETF RFC 1035 [19]. Each label shall begin and end with either an alphabetic character or a digit in accordance with IETF RFC 1123 [20]. The case of alphabetic characters is not significant.

During the MBMS service activation in roaming scenario, the BM-SC in the visited network shall derive the home network domain name from the IMSI as described in the following steps:

1. Take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used (see 3GPP TS 31.102 [27], 3GPP TS 51.011 [66]) and separate them into MCC and MNC; if the MNC is 2 digits then a zero shall be added at the beginning;
2. Use the MCC and MNC derived in step 1 to create the "mnc<MNC>.mcc<MCC>.3gppnetwork.org" realm name;
3. Add the label "mbms." to the beginning of the realm name.

An example of a home realm used in the MBMS roaming case is:

IMSI in use: 234150999999999;

Where:

MCC = 234;

MNC = 15;

MSIN = 0999999999

Which gives the home network realm: mbms.mnc015.mcc234.3gppnetwork.org.

15.5 Addressing and identification for Bootstrapping MBMS Service Announcement

The UE needs a Service Announcement Fully Qualified Domain Name (FQDN) to bootstrap MBMS Service Announcement as specified in 3GPP TS 26.346 [105].

The Service Announcement FQDN is composed of six labels. The last three labels shall be "pub.3gppnetwork.org". The second and third labels together shall uniquely identify the PLMN. The first label shall be "mbmsbs".

The Service Announcement FQDN is derived from the IMSI or Visited PLMN Identity as follows:

"mbmsbs.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org"

where:

"mnc" and "mcc" serve as invariable identifiers for the following digits.

- When using the Service Announcement FQDN in a visited network, the <MNC> and <MCC> shall be derived from the visited PLMN Identity as defined in clause 12.1.
- When using the Service Announcement FQDN in the home network, the <MNC> and <MCC> shall be derived from the components of the IMSI as defined in clause 2.2.

In order to guarantee inter-PLMN DNS translation, the <MNC> and <MCC> coding used in the "mbmsbs.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org" format of the Service Announcement FQDN shall be:

- <MNC> = 3 digits
- <MCC> = 3 digits

If there are only 2 significant digits in the MNC, one "0" digit shall be inserted at the left side to fill the 3 digits coding of MNC in the Service Announcement FQDN.

As an example, the Service Announcement FQDN for MCC 345 and MNC 12 is coded in the DNS as:

"mbmsbs.mnc012.mcc345.pub.3gppnetwork.org".

16 Numbering, addressing and identification within the GAA subsystem

16.1 Introduction

This clause describes the format of the parameters needed to access the GAA system. For further information on the use of the parameters see 3GPP TS 33.221 [58]. For more information on the ".3gppnetwork.org" domain name and its applicability, see Annex D of the present document.

16.2 BSF address

The Bootstrapping Server Function (BSF) address is in the form of a Fully Qualified Domain Name as defined in IETF RFC 1035 [19] and IETF RFC 1123 [20]. The BSF address consists of one or more labels. Each label shall consist of the alphabetic characters (A-Z and a-z), digits (0-9) and the hyphen (-) in accordance with IETF RFC 1035 [19]. Each label shall begin and end with either an alphabetic character or a digit in accordance with IETF RFC 1123 [20]. The case of alphabetic characters is not significant.

For 3GPP systems, the UE shall discover the BSF address from the identity information related to the UICC application that is used during the bootstrapping procedure i.e. IMSI for USIM, or IMPI for ISIM, in the following way:

- In the case where the USIM is used in bootstrapping, the BSF address shall be derived as follows:
  1. take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used (see 3GPP TS 31.102 [27]) and separate them into MCC and MNC; if the MNC is 2 digits then a zero shall be added at the beginning;
  2. use the MCC and MNC derived in step 1 to create the "mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org" domain name;
  3. add the label "bsf." to the beginning of the domain.

  Example 1: If IMSI in use is "234150999999999", where MCC=234, MNC=15, and MSIN=0999999999, the BSF address would be "bsf.mnc015.mcc234.pub.3gppnetwork.org".
- In the case where ISIM is used in bootstrapping, the BSF address shall be derived as follows:
  1. extract the domain name from the IMPI;
  2. if the last two labels of the domain name extracted from the IMPI are "3gppnetwork.org":

a. the first label is "bsf";

b. the next labels are all labels of the domain name extracted from the IMPI apart from the last two labels; and

c. the last three labels are "pub.3gppnetwork.org";

Example 2: If the IMPI in use is "234150999999999@ims.mnc015.mcc234.3gppnetwork.org", the BSF address would be "bsf.ims.mnc015.mcc234.pub.3gppnetwork.org".

3. if the last two labels of the domain name extracted from the IMPI are other than the "3gppnetwork.org":

a. add the label "bsf." to the beginning of the domain.

Example 3: If the IMPI in use is "user@operator.com", the BSF address would be "bsf.operator.com ".

17 Numbering, addressing and identification within the Generic Access Network

17.1 Introduction

This clause describes the format of the parameters needed to access the Generic Access Network (GAN). For further information on the use of the parameters and GAN in general, see 3GPP TS 43.318 [61] and 3GPP TS 44.318 [62]. For more information on the ".3gppnetwork.org" domain name and its applicability, see Annex D of the present document.

17.2 Network Access Identifiers

17.2.1 Home network realm

The home network realm shall be in the form of an Internet domain name, e.g. operator.com, as specified in IETF RFC 1035 [19] and IETF RFC 1123 [20]. The home network realm consists of one or more labels. Each label shall consist of the alphabetic characters (A-Z and a-z), digits (0-9) and the hyphen (-) in accordance with IETF RFC 1035 [19]. Each label shall begin and end with either an alphabetic character or a digit in accordance with IETF RFC 1123 [20]. The case of alphabetic characters is not significant.

The UE shall derive the home network realm from the IMSI as described in the following steps:

1. take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used (see 3GPP TS 31.102 [27], 3GPP TS 51.011 [66]) and separate them into MCC and MNC; if the MNC is 2 digits then a zero shall be added at the beginning;
2. use the MCC and MNC derived in step 1 to create the "mnc<MNC>.mcc<MCC>.3gppnetwork.org" network realm;
3. add the label "gan." to the beginning of the network realm.

An example of a home network realm is:

IMSI in use: 234150999999999;

Where:

MCC = 234;

MNC = 15;

MSIN = 0999999999,

Which gives the home network realm: gan.mnc015.mcc234.3gppnetwork.org.

NOTE: If it is not possible for the UE to identify whether a 2 or 3 digit MNC is used (e.g. SIM is inserted and the length of MNC in the IMSI is not available in the "Administrative data" data file), it is implementation dependent how the UE determines the length of the MNC (2 or 3 digits).

17.2.2 Full Authentication NAI

The Full Authentication NAI in both EAP-SIM and EAP-AKA shall take the form of an NAI as specified in clause 2.1 of IETF RFC 4282 [53]. The format of the Full Authentication NAI shall comply with IETF RFC 4187 [50] when EAP-AKA authentication is used and with IETF RFC 4186 [51], when EAP-SIM authentication is used. The realm used shall be a home network realm as defined in clause 17.2.1.

The result will therefore be an identity of the form:

"0<IMSI>@gan.mnc<MNC>.mcc<MCC>.3gppnetwork.org", for EAP-AKA authentication and
"1<IMSI>@gan.mnc<MNC>.mcc<MCC>.3gppnetwork.org", for EAP-SIM authentication

EXAMPLE 1: For EAP AKA authentication: If the IMSI is 234150999999999 (MCC = 234, MNC = 15), the Full Authentication NAI takes the form 0234150999999999@gan.mnc015.mcc234.3gppnetwork.org.

EXAMPLE 2: For EAP SIM authentication: If the IMSI is 234150999999999 (MCC = 234, MNC = 15), the Full Authentication NAI takes the form 1234150999999999@gan.mnc015.mcc234.3gppnetwork.org.

17.2.3 Fast Re-authentication NAI

The Fast Re-authentication NAI in both EAP-SIM and EAP-AKA shall take the form of an NAI as specified in clause 2.1 of IETF RFC 4282 [53]. The UE shall use the re-authentication identity received during the previous EAP-SIM or EAP-AKA authentication procedure. If such an NAI contains a realm part then the UE should not modify it, otherwise it shall use a home network realm as defined in sub clause 17.2.1.

The result will therefore be an identity of the form:

"<re-authentication_ID_username>@<re-authentication_ID_realm> for both EAP-SIM and EAP-AKA authentication when a realm is present in the re-authentication identity received during the previous EAP-SIM or EAP-AKA authentication procedure and

"<re-authentication_ID_username>@gan.mnc<MNC>.mcc<MCC>.3gppnetwork.org", for both EAP-SIM and EAP-AKA authentication when a realm is *not* present in the re-authentication identity received during the previous EAP-SIM or EAP-AKA authentication procedure.

EXAMPLE 1: If the re-authentication identity is "12345" and the IMSI is 234150999999999 (MCC = 234, MNC = 15), the Fast Re-authentication NAI takes the form 12345@gan.mnc015.mcc234.3gppnetwork.org

EXAMPLE 2: If the re-authentication identity is "12345@aaa1.gan.mnc015.mcc234.3gppnetwork.org", the Fast Re-authentication NAI takes the form 12345@aaa1.gan.mnc015.mcc234.3gppnetwork.org

17.3 Node Identifiers

17.3.1 Home network domain name

The home network domain name shall be in the form of an Internet domain name, e.g. operator.com, as specified in IETF RFC 1035 [19] and IETF RFC 1123 [20]. The home network domain name consists of one or more labels. Each label shall consist of the alphabetic characters (A-Z and a-z), digits (0-9) and the hyphen (-) in accordance with IETF RFC 1035 [19]. Each label shall begin and end with either an alphabetic character or a digit in accordance with IETF RFC 1123 [20]. The case of alphabetic characters is not significant.

The UE shall derive the home network domain name from the IMSI as described in the following steps:

1. take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used (see 3GPP TS 31.102 [27], 3GPP TS 51.011 [66]) and separate them into MCC and MNC; if the MNC is 2 digits then a zero shall be added at the beginning;

2. use the MCC and MNC derived in step 1 to create the "mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org" domain name;

3. add the label "gan." to the beginning of the domain name.

An example of a home network domain name is:

IMSI in use: 234150999999999;

Where:

MCC = 234;

MNC = 15;

MSIN = 0999999999,

Which gives the home network domain name: gan.mnc015.mcc234.pub.3gppnetwork.org.

NOTE: If it is not possible for the UE to identify whether a 2 or 3 digit MNC is used (e.g. SIM is inserted and the length of MNC in the IMSI is not available in the "Administrative data" data file), it is implementation dependent how the UE determines the length of the MNC (2 or 3 digits).

17.3.2 Provisioning GANC-SEGW identifier

The Provisioning GANC-SEGW identifier shall take the form of a fully qualified domain name (FQDN) as specified in IETF RFC 1035 [19] and IETF RFC 1123 [20]. The Provisioning GANC-SEGW identifier consists of one or more labels. Each label shall consist of the alphabetic characters (A-Z and a-z), digits (0-9) and the hyphen (-) in accordance with IETF RFC 1035 [19]. Each label shall begin and end with either an alphabetic character or a digit in accordance with IETF RFC 1123 [20]. The case of alphabetic characters is not significant.

If the (U)SIM is not provisioned with the FQDN or IP address of the Provisioning GANC-SEGW, the UE derives an FQDN from the IMSI to identify the Provisioning GANC-SEGW. The UE shall derive such an FQDN as follows:

1. create a domain name as specified in 17.3.1;

2. add the label "psegw." to the beginning of the domain name.

An example of an FQDN for a Provisioning GANC-SEGW is:

IMSI in use: 234150999999999;

Where:

MCC = 234;

MNC = 15;

MSIN = 0999999999,

Which gives the FQDN: psegw.gan.mnc015.mcc234.pub.3gppnetwork.org.

NOTE: If it is not possible for the UE to identify whether a 2 or 3 digit MNC is used (e.g. SIM is inserted and the length of MNC in the IMSI is not available in the "Administrative data" data file), it is implementation dependent how the UE determines the length of the MNC (2 or 3 digits).

17.3.3 Provisioning GANC identifier

The Provisioning GANC identifier shall take the form of a fully qualified domain name (FQDN) as specified in IETF RFC 1035 [19] and IETF RFC 1123 [20]. The Provisioning GANC identifier consists of one or more labels. Each label shall consist of the alphabetic characters (A-Z and a-z), digits (0-9) and the hyphen (-) in accordance with IETF RFC 1035 [19]. Each label shall begin and end with either an alphabetic character or a digit in accordance with IETF RFC 1123 [20]. The case of alphabetic characters is not significant.

If the (U)SIM is not provisioned with the FQDN or IP address of the Provisioning GANC, the UE derives an FQDN from the IMSI to identify the Provisioning GANC. The UE shall derive such an FQDN as follows:

1. create a domain name as specified in 17.3.1;
2. add the label "pganc." to the beginning of the domain name.

An example of an FQDN for a Provisioning GANC is:

IMSI in use: 234150999999999;

Where:

MCC = 234;

MNC = 15;

MSIN = 0999999999,

Which gives the FQDN: pganc.gan.mnc015.mcc234.pub.3gppnetwork.org.

NOTE: If it is not possible for the UE to identify whether a 2 or 3 digit MNC is used (e.g. SIM is inserted and the length of MNC in the IMSI is not available in the "Administrative data" data file), it is implementation dependent how the UE determines the length of the MNC (2 or 3 digits).

18 Addressing and Identification for IMS Service Continuity and Single-Radio Voice Call Continuity

18.1 Introduction

This clause describes the format of the parameters needed for the support of IMS Service Continuity. For further information on the use of the parameters see 3GPP TS 23.237 [71] and also 3GPP TS 23.292 [70].

18.2 CS Domain Routeing Number (CSRN)

A CS Domain Routeing Number (CSRN) is a number that is used to route a call from the IM CN subsystem to the user in the CS domain. The structure is as defined in clause 3.4.

18.3 IP Multimedia Routeing Number (IMRN)

An IP Multimedia Routeing Number (IMRN) is a routable number that points to the IM CN subsystem. In a roaming scenario, the IMRN has the same structure as an international ISDN number (see clause 3.4). The Tel URI format of the IMRN (see IETF RFC 3966 [45]) is treated as a PSI (see clause 13.5) within the IM CN subsystem.

18.4 Session Transfer Number (STN)

A Session Transfer Number (STN) is a public telecommunication number, as defined by ITU-T Recommendation E.164 [10] and is used by the UE to request Session Transfer of the media path from PS to CS access.

18.5 Session Transfer Identifier (STI)

A Session Transfer Identifier (STI) is a SIP URI or SIP dialogue ID (see IETF RFC 3261 [26] for more information) and is used by the UE to request Session Transfer of a media path.

18.6 Session Transfer Number for Single Radio Voice Call Continuity (STN-SR)

The Session Transfer Number for Single Radio Voice Call Continuity (STN-SR) is a public telecommunication number, as defined by ITU-T Recommendation E.164 [10] and is used by the MSC Server to request session transfer of the media path from the PS domain to CS domain.

18.7 Correlation MSISDN

A Correlation MSISDN (C-MSISDN) is an MSISDN (see clause 3.3) that is used for correlation of sessions at access transfer and to route a call from the IM CN subsystem to the same user in the CS domain. The C-MSISDN is equal to the MSISDN or the basic MSISDN if multinumbering option is used (see 3GPP TS 23.008 [2], clause 2.1.3) of the CS access. Any MSISDN of a user that can be used for TS11 (telephony) in the CS domain which is not shared by more than one IMS Private Identity in an IMS CN subsystem, can serve as the user's C-MSISDN.

The C-MSISDN is bound to the IMS Private User Identity and is uniquely assigned per IMSI and IMS Private User Identity.

If A-MSISDN is available it shall be used as the C-MSISDN. For the definition of A-MSISDN refer to clause 18.9.

18.8 Transfer Identifier for CS to PS Single Radio Voice Call Continuity (STI-rSR)

A Session Transfer Identifier for CS to PS Single Radio Voice Call Continuity (STI-rSR) is a SIP URI (see IETF RFC 3261 [26] for more information) and is used by the UE to request access transfer of a media path.

18.9 Additional MSISDN

An Additional MSISDN (A-MSISDN) is an MSISDN (see clause 3.3) that is assigned to a user with PS subscription in addition to the already assigned MSISDN(s).

The structure of an A-MSISDN should follow the structure of an MSISDN number as defined in clause 3.3.

The A-MSISDN shall be able to be used for TS11 (telephony) in the CS domain and shall be uniquely assigned per IMSI.

19 Numbering, addressing and identification for the Evolved Packet Core (EPC)

19.1 Introduction

This clause describes the format of the parameters needed to access the Enhanced Packet Core (EPC). For further information on the use of the parameters see 3GPP TS 23.401 [72] and 3GPP TS 23.402 [68]. For more information on the ".3gppnetwork.org" domain name and its applicability, see Annex D of the present document

19.2 Home Network Realm/Domain

The home Network Realm/Domain shall be in the form of an Internet domain name, e.g. operator.com, as specified in IETF RFC 1035 [19] and IETF RFC 1123 [20]. The home Network Realm/Domain consists of one or more labels. Each label shall consist of the alphabetic characters (A-Z and a-z), digits (0-9) and the hyphen (-) in accordance with IETF RFC 1035 [19]. Each label shall begin and end with either an alphabetic character or a digit in accordance with IETF RFC 1123 [20]. The case of alphabetic characters is not significant.

The Home Network Realm/Domain shall be in the form of "epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org", where "<MNC>" and "<MCC>" fields correspond to the MNC and MCC of the operator's PLMN. Both the "<MNC>" and "<MCC>" fields are 3 digits long. If the MNC of the PLMN is 2 digits, then a zero shall be added at the beginning.

For example, the Home Network Realm/Domain of an IMSI shall be derived as described in the following steps:

1. take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used (see 3GPP TS 31.102 [27]) and separate them into MCC and MNC; if the MNC is 2 digits then a zero shall be added at the beginning;
2. use the MCC and MNC derived in step 1 to create the "mnc<MNC>.mcc<MCC>.3gppnetwork.org" domain name;
3. add the label "epc" to the beginning of the domain name.

An example of a Home Network Realm/Domain is:

IMSI in use: 234150999999999;

Where:

MCC = 234;

MNC = 15;

MSIN = 0999999999;

Which gives the Home Network Realm/Domain name: epc.mnc015.mcc234.3gppnetwork.org.

NOTE: If it is not possible for a UE to identify whether a 2 or 3 digit MNC is used (e.g. USIM is inserted and the length of MNC in the IMSI is not available in the "Administrative data" data file), it is implementation dependent how the UE determines the length of the MNC (2 or 3 digits).

19.3 3GPP access to non-3GPP access interworking

19.3.1 Introduction

This clause describes the format of the UE identification needed to access the 3GPP EPC from both 3GPP and non-3GPP accesses.

The NAI is generated respectively by the S-GW at the S5/S8 reference point and by the UE for the S2a, S2b and S2c reference points.

The NAI shall be generated as follows:

- based on the IMSI when the UE is performing a non-emergency Attach;
- based on the IMEI when the UE is performing an emergency attach and IMSI is not available (see clause 19.3.6); or
- based on the IMSI or the IMEI (depending on the interface and information element) when the UE is performing an emergency attach and IMSI is available in the UE, as follows:
  - a UE that has an IMSI shall construct an Emergency NAI based on IMSI (see clause 4.6.1 of 3GPP TS 23.402 [68] and clause 19.3.9 of this specification);
  - if the IMSI is not authenticated by the network, the network requests the IMEI from the UE and the network shall then construct a NAI based on the IMEI for identifying the user in the EPC (see 3GPP TS 29.273 [78]).

For further information on the use of the parameters see the clauses below and 3GPP TS 33.402 [69] and 3GPP TS 29.273 [78].

19.3.2 Root NAI

The Root NAI shall take the form of an NAI, and shall have the form username@realm as specified in clause 2.1 of IETF RFC 4282 [53].

When the username part is the IMSI, the realm part of Root NAI shall be built according to the following steps:

1. Convert the leading digits of the IMSI, i.e. MNC and MCC, into a domain name, as described in clause 19.2.
2. Prefix domain name with the label of "nai".

The resulting realm part of the Root NAI will be in the form:

"@nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org"

When including the IMSI, the Root NAI is prepended with a specific leading digit when used for EAP authentication (see 3GPP TS 29.273 [78]) in order to differentiate between EAP authentication method. The leading digit is:

- "0" when used in EAP-AKA, as specified in IETF RFC 4187 [50]
- "6" when used in EAP-AKA', as specified in IETF RFC 5448 [82].

The resulting Root NAI will be in the form:

"0<IMSI>@nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org" when used for EAP AKA authentication

"6<IMSI>@nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org" when used for EAP AKA' authentication

For example, if the IMSI is 234150999999999 (MCC = 234, MNC = 15), the Root NAI takes the form 0234150999999999@nai.epc.mnc015.mcc234.3gppnetwork.org for EAP AKA authentication and the Root NAI takes the form 6234150999999999@nai.epc.mnc015.mcc234.3gppnetwork.org for EAP AKA' authentication.

The NAI sent in the Mobile Node Identifier field in PMIPv6 shall not include the digit prepended in front of the IMSI based username that is described above.

19.3.3 Decorated NAI

The Decorated NAI shall take the form of a NAI and shall have the form 'homerealm!username@otherrealm' or 'Visitedrealm!homerealm!username@otherrealm' as specified in clause 2.7 of the IETF RFC 4282 [53].

The realm part of Decorated NAI consists of 'otherrealm', see the IETF RFC 4282 [53]. 'Homerealm' is the realm as specified in clause 19.2, using the HPLMN ID ('homeMCC' + 'homeMNC)'. 'Visitedrealm' is the realm built using the VPLMN ID ('VisitedMCC' + 'VisitedMNC)', 'Otherrealm' is:

- the realm built using the PLMN ID (visitedMCC + visited MNC) if the service provider selected as a result of the service provider selection (see 3GPP TS 24.302 [77]) has a PLMN ID; or
- a domain name of a service provider if the selected service provider does not have a PLMN ID (3GPP TS 24.302 [77]).

When the username part of Decorated NAI includes the IMSI and the service provider has a PLMN ID, the Decorated NAI shall be built following the same steps as specified for Root NAI in clause 19.3.2.

The result will be a decorated NAI of the form:

- nai.epc.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org !0<IMSI>@nai.epc.mnc<visitedMNC>.mcc<visitedMCC>.3gppnetwork.org for EAP AKA authentication.

or

- nai.epc.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org !6<IMSI>@nai.epc.mnc<visitedMNC>.mcc<visitedMCC>.3gppnetwork.org for EAP AKA' authentication.

For example, if the service provider has a PLMN ID and the IMSI is 234150999999999 (MCC = 234, MNC = 15) and the PLMN ID of the Selected PLMN is MCC = 610, MNC = 71, then the Decorated NAI takes the form either as:

- nai.epc.mnc015.mcc234.3gppnetwork.org!0234150999999999@nai.epc.mnc071.mcc610.3gppnetwork.org for EAP AKA authentication

or

- nai.epc.mnc015.mcc234.3gppnetwork.org!6234150999999999@nai.epc.mnc071.mcc610.3gppnetwork.org for EAP AKA' authentication.

For example, if the domain name of a service provider is 'realm.org' and IMSI-based permanent username is used, then the Decorated NAI takes the form either as:

- nai.epc.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org !0<IMSI>@realm.org for EAP AKA authentication

or

- nai.epc.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org !6<IMSI>@realm.org for EAP AKA' authentication.

If the UE has selected a WLAN that directly interworks with a service provider in the Equivalent Visited Service Providers (EVSP) list provided by the RPLMN, see 3GPP TS 23.402 [77], clause 4.8.2b, then the decorated NAI is constructed to include the realm of this service provider and the realm of RPLMN. If the domain name of a service provider is 'realm.org' and IMSI-based permanent username is used, then the Decorated NAI with double decoration takes the form either as:

- nai.epc.mnc<rplmnMNC>.mcc<rplmnMCC>.3gppnetwork.org !nai.epc.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org!0<IMSI>@realm.org for EAP AKA authentication

or

- nai.epc.mnc<rplmnMNC>.mcc<rplmnMCC>.3gppnetwork.org !nai.epc.mnc<homeMNC>.mcc<homeMCC>.3gppnetwork.org!6<IMSI>@realm.org for EAP AKA' authentication.

When the username part of Decorated NAI includes a Fast Re-authentication NAI, the Decorated NAI shall be built following the same steps as specified for the Fast Re-authentication NAI in clause 19.3.4.

When the username part of Decorated NAI includes a Pseudonym, the Decorated NAI shall be built following the same steps as specified for the Pseudonym identity in clause 19.3.5.

19.3.4 Fast Re-authentication NAI

The Fast Re-authentication NAI shall take the form of a NAI as specified in clause 2.1 of IETF RFC 4282 [53]. If the 3GPP AAA server does not return a complete NAI, the Fast Re-authentication NAI shall consist of the username part of the fast re-authentication identity as returned from the 3GPP AAA server and the same realm as used in the permanent user identity. If the 3GPP AAA server returns a complete NAI as the re-authentication identity, then this NAI shall be used. The username part of the fast re-authentication identity shall be decorated as described in 19.3.3 if the Selected PLMN is different from the HPLMN.

For EAP-AKA authentication, the username portion of the fast re-authentication identity shall be prepended with the single digit "4" as specified in clause 4.1.1.7 of IETF RFC 4187 [50].

For EAP AKA', see IETF RFC 5448 [82], the Fast Re-authentication NAI shall comply with IETF RFC 4187 [50] except that the username part of the NAI shall be prepended with single digit "8".

NOTE: The permanent user identity is either the Root NAI or Decorated NAI as defined in clauses 19.3.2 and 19.3.3, respectively.

EXAMPLE 1: If the fast re-authentication identity returned by the 3GPP AAA Server is 358405627015, the IMSI is 234150999999999 (MCC = 234, MNC = 15) and EAP-AKA is used, the Fast Re-authentication NAI for the case when NAI decoration is not used takes the form: 4358405627015@nai.epc.mnc015.mcc234.3gppnetwork.org

EXAMPLE 2: If the fast re-authentication identity returned by the 3GPP AAA Server is "358405627015@aaa1.nai.epc.mnc015.mcc234.3gppnetwork.org" , the IMSI is 234150999999999 (MCC = 234, MNC = 15) and EAP-AKA' is used, the Fast Re-authentication NAI for the case when NAI decoration is not used takes the form: 8358405627015@aaa1.nai.epc.mnc015.mcc234.3gppnetwork.org

EXAMPLE 3: If the fast re-authentication identity returned by the 3GPP AAA Server is 358405627015, the IMSI is 234150999999999 (MCC = 234, MNC = 15), the PLMN ID of the Selected PLMN is MCC = 610, MNC = 71 and EAP-AKA is used, the Fast Re-authentication NAI takes the form: nai.epc.mnc015.mcc234.3gppnetwork.org !4358405627015@nai.epc.mnc071.mcc610.3gppnetwork.org.

19.3.5 Pseudonym Identities

The pseudonym shall take the form of an NAI, as specified in clause 2.1 of IETF RFC 4282 [53].

The pseudonym shall be generated as specified in clause 6.4.1 of 3GPP TS 33.234 [55]. This part of the pseudonym shall follow the UTF-8 transformation format specified in IETF RFC 2279 [54] except for the following reserved hexadecimal octet value:

FF

When the pseudonym username is coded with FF, this reserved value is used to indicate the special case when no valid temporary identity exists in the UE (see 3GPP TS 24.234 [48] for more information). The network shall not allocate a temporary identity with the whole username coded with the reserved hexadecimal value FF.

The username portion of the pseudonym identity shall be prepended with the single digit "2" as specified in clause 4.1.1.7 of IETF RFC 4187 [50] for EAP-AKA. For EAP AKA', see IETF RFC 5448 [82], the pseudonym NAI shall comply with IETF RFC 4187 [50] except that the username part of the NAI shall be prepended with single digit "7".

NOTE: The permanent user identity is either the Root NAI or Decorated NAI as defined in clauses 19.3.2 and 19.3.3, respectively.

EXAMPLE 1: For EAP AKA, if the pseudonym returned by the 3GPP AAA Server is 258405627015 and the IMSI is 234150999999999 (MCC = 234, MNC = 15), the pseudonym NAI for the case when NAI decoration is not used takes the form: 258405627015@nai.epc.mnc015.mcc234.3gppnetwork.org

EXAMPLE 2: For EAP AKA', if the pseudonym returned by the 3GPP AAA Server is 758405627015 and the IMSI is 234150999999999 (MCC = 234, MNC = 15), the pseudonym NAI for the case when NAI decoration is not used takes the form: 758405627015@nai.epc.mnc015.mcc234.3gppnetwork.org

EXAMPLE 3: For EAP AKA, if the pseudonym returned by the 3GPP AAA Server is 258405627015 and the IMSI is 234150999999999 (MCC = 234, MNC = 15), and the PLMN ID of the Selected PLMN is MCC = 610, MNC = 71, the pseudonym NAI takes the form: nai.epc.mnc015.mcc234.3gppnetwork.org! 258405627015@nai.epc.mnc071.mcc610.3gppnetwork.org

EXAMPLE 4: For EAP AKA', if the pseudonym returned by the 3GPP AAA Server is 758405627015 and the IMSI is 234150999999999 (MCC = 234, MNC = 15), and the PLMN ID of the Selected PLMN is MCC = 610, MNC = 71, the pseudonym NAI takes the form: nai.epc.mnc015.mcc234.3gppnetwork.org! 758405627015@nai.epc.mnc071.mcc610.3gppnetwork.org

19.3.6 Emergency NAI for Limited Service State

This clause describes the format of the UE identification needed to access the 3GPP EPC from both 3GPP and non-3GPP accesses, when UE is performing an emergency attach and IMSI is not available or not authenticated (see clause 19.3.1). For more information, see clauses 4.6.1 and 5.2 of 3GPP TS 23.402 [68].

The Emergency NAI for Limited Service State shall take the form of an NAI, and shall have the form username@realm as specified in clause 2.1 of IETF RFC 4282 [53]. The exact format shall be:

imei<IMEI>@sos.invalid

NOTE: The top level domain ".invalid" is a reserved top level domain, as specified in IETF RFC 2606 [64], and is used here due to the fact that this NAI never needs to be resolved for routing (as specified in 3GPP TS 23.402 [68]).

or

mac<MAC>@sos.invalid

For example, if the IMEI is 219551288888888, the Emergency NAI for Limited Service State then takes the form of imei219551288888888@sos.invalid.

For example, if the MAC address is 44-45-53-54-00-AB, the Emergency NAI for Limited Service State then takes the form of mac4445535400AB@sos.invalid, where the MAC address is represented in hexadecimal format without separators.

19.3.7 Alternative NAI

The Alternative NAI shall take the form of a NAI, i.e. 'any_username@REALM' as specified of IETF RFC 4282 [53]. The Alternative NAI shall not be routable from any AAA server.

The Alternative NAI shall contain a username part which is not derived from the IMSI. The username part shall not be a null string.

The REALM part of the NAI shall be "unreachable.3gppnetwork.org".

The result shall be an NAI in the form of:

"<any_non_null_string>@unreachable.3gppnetwork.org".

19.3.8 Keyname NAI

The keyname NAI shall take the form of an NAI, and shall have the form username@realm as specified in clause 2.1 of IETF RFC 4282 [53].

The username part is the EMSK name as defined in IETF RFC 6696 [113].

For ERP exchange with an ER server located in the 3GPP AAA Server, the realm part of the keyname NAI shall be the realm part of the Root NAI of the UE as described in clause 19.3.2, i.e. the realm part of the keyName-NAI will be in the form:

"@nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org"

For ERP exchange with an ER server located in the TWAP or in the 3GPP AAA Proxy, the realm part of the keyname NAI shall be the realm discovered by the UE in the non-3GPP access network (received at the lower layer or through an ERP exchange as described in IETF RFC 6696 [113]).

19.3.9 IMSI-based Emergency NAI

This clause describes the format of the UE identification needed to access the 3GPP EPC from non-3GPP accesses, when UE is performing an emergency attach and IMSI is available. For more information, see clause 4.4.1 of 3GPP TS 24.302 [77].

The IMSI-based Emergency NAI shall take the form of an NAI and shall be encoded as the Root NAI as specified in clause 19.3.2, but with the realm name prepended by the "sos" label. The resulting realm part of the IMSI-based Emergency NAI will be in the form:

"@sos.nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org"

The resulting IMSI-based Emergency NAI will be in the form:

"0<IMSI>@sos.nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org" when used for EAP AKA authentication

"6<IMSI>@sos.nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org" when used for EAP AKA' authentication

For example, if the IMSI is 234150999999999 (MCC = 234, MNC = 15), the IMSI-based Emergency NAI takes the form 0234150999999999@sos.nai.epc.mnc015.mcc234.3gppnetwork.org for EAP AKA authentication and it takes the form 6234150999999999@sos.nai.epc.mnc015.mcc234.3gppnetwork.org for EAP AKA' authentication.

19.4 Identifiers for Domain Name System procedures

19.4.1 Introduction

This clause describes Domain Name System (DNS) related identifiers used by the procedures specified in 3GPP TS 29.303 [73].

The DNS identifiers for APNs for legacy systems (as defined in clause 9), RAIs (as defined in clause C.1, GSNs (as defined in clause C.2) and RNCs (as defined in clause C.3) in the present document use the top level domain ".gprs" and have a similar purpose and function as those described below. These clauses are still valid and DNS records based on these and the below types of identifiers are expected to coexist in an operator's network for the purpose of backwards compatibility and interworking with legacy networks.

The APN as defined in clause 9 is used also in EPC to identify the access network to be used for a specific PDN connection or PDP Context. In addition, the APN Network Identifier (APN-NI) part of the APN as defined in clause 9.1.1 of the present document may be used to access a service associated with a PDN-GW or GGSN. This is achieved by defining an APN which in addition to being usable to select a PDN-GW or GGSN is locally interpreted by the PDN-GW or GGSN as a request for a specific service.

For DNS procedures defined in 3GPP TS 29.303 [73], an APN-FQDN derived from a given APN is used instead of the APN itself as defined in clause 19.4.2.2. For all other purposes, including communication between EPC nodes and to the UE, the APN format defined in clause 9 is used. In order to support backwards compatibility with existing GPRS/PS roaming using the Gn/Gp interfaces, the APN as specified in clause 9 of the present document may also be used for the DNS procedures as defined in 3GPP TS 23.060 [3].

19.4.2 Fully Qualified Domain Names (FQDNs)

19.4.2.1 General

The encoding of any identifier used as part of a Fully Qualifed Domain Name (FQDN) shall follow the Name Syntax defined in IETF RFC 2181 [18], IETF RFC 1035 [19] and IETF RFC 1123 [20]. An FQDN consists of one or more labels. Each label is coded as a one octet length field followed by that number of octets coded as 8 bit ASCII characters. Following IETF RFC 1035 [19] the labels shall consist only of the alphabetic characters (A-Z and a-z), digits (0-9) and the hyphen (-). Following IETF RFC 1123 [20], the label shall begin and end with either an alphabetic character or a digit. The case of alphabetic characters is not significant. Identifiers are not terminated by a length byte of zero.

NOTE: A length byte of zero is added by the querying entity at the end of the FQDN before interrogating a DNS server.

For the purpose of presentation, identifiers are usually displayed as a string in which the labels are separated by dots (e.g. "Label1.Label2.Label3").

19.4.2.2 Access Point Name FQDN (APN-FQDN)

19.4.2.2.1 Structure

The Access Point Name FQDN (APN-FQDN) is derived from an APN as follows. The APN consists of an APN Network Identifier (APN-NI) and an APN Operator Identifier (APN-OI), which are as defined in clause 9.1.1 and 9.1.2 of the present document.

If an APN is constructed using the default APN-OI, the APN-FQDN shall be obtained from the APN by inserting the labels "apn.epc." between the APN-NI and the default APN - OI, and by replacing the label ".gprs" at the end of the default APN-OI with the labels ".3gppnetwork.org".

EXAMPLE1: For an APN of internet.mnc015.mcc234.gprs, the derived APN-FQDN is internet.apn.epc.mnc015.mcc234.3gppnetwork.org

If an APN is constructed using the APN-OI Replacement field (as defined in 3GPP TS 23.060 [3] and 3GPP TS 23.401 [72]), the APN-FQDN shall be obtained from the APN by inserting the labels "apn.epc." between the label "mnc<MNC>" and its preceding label, and by replacing the label ".gprs" at the end of the APN-OI Replacement field with the labels ".3gppnetwork.org".

EXAMPLE 2: If an APN-OI Replacement field is province1.mnc015.mcc234.gprs and an APN-NI is internet, the derived APN-FQDN is internet. province1.apn.epc.mnc015.mcc234.3gppnetwork.org

19.4.2.2.2 Void

19.4.2.2.3 Void

19.4.2.2.4 Void

19.4.2.3 Tracking Area Identity (TAI)

The Tracking Area Identity (TAI) consists of a Mobile Country Code (MCC), Mobile Network Code (MNC), and Tracking Area Code (TAC). It is composed as shown in figure 19.4.2.3.1.

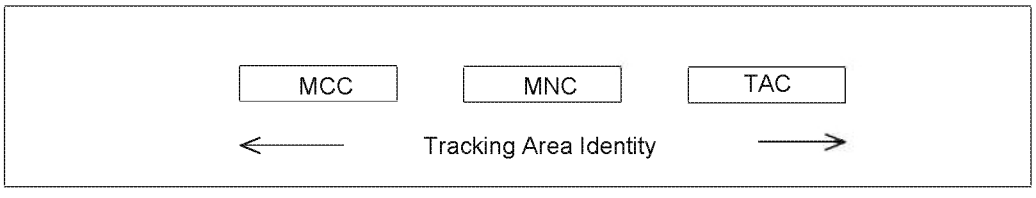

Figure 19.4.2.3.1: Structure of the Tracking Area Identity (TAI)

The TAI is composed of the following elements:

- Mobile Country Code (MCC) identifies the country in which the PLMN is located. The value of the MCC is the same as the three digit MCC contained in the IMSI;
- Mobile Network Code (MNC) is a code identifying the PLMN in that country. The value of the MNC is the same as the two or three digit MNC contained in the IMSI;
- Tracking Area Code (TAC) is a fixed length code (of 2 octets) identifying a Tracking Area within a PLMN. This part of the tracking area identification shall be coded using a full hexadecimal representation. The following are reserved hexadecimal values of the TAC:
  - 0000, and
  - FFFE.

NOTE: The above reserved values are used in some special cases when no valid TAI exists in the MS (see 3GPP TS 24.301 [90] for more information).

A subdomain name can be derived from the TAI. This shall be done by adding the label "tac" to the beginning of the Home Network Realm/Domain (see clause 19.2) and encoding the TAC as a sub-domain. This is called the TAI FQDN..

The TAI FQDN shall be constructed as follows:

tac-lb<TAC-low-byte>.tac-hb<TAC-high-byte>.tac.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

The TAC is a 16-bit integer. The <TAC-high-byte> is the hexadecimal string of the most significant byte in the TAC and the <TAC-low-byte > is the hexadecimal string of the least significant byte. If there are less than 2 significant digits in <TAC-high-byte> or <TAC-low-byte >, "0" digit(s) shall be inserted at the left side to fill the 2 digit coding.

19.4.2.4 Mobility Management Entity (MME)

A Mobility Management Entity (MME) within an operator's network is identified using a MME Group ID (MMEGI), and an MME Code (MMEC).

A subdomain name shall be derived from the MNC and MCC by adding the label "mme" to the beginning of the Home Network Realm/Domain (see clause 19.2).

The MME node FQDN shall be constructed as:

mmec<MMEC>.mmegi<MMEGI>.mme.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

Where <MMEC> and <MMEGI> are the hexadecimal strings of the MMEC and MMEGI.

An MME pool FQDN shall be constructed as:

mmegi<MMEGI>.mme.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

If there are less than 2 significant digits in <MMEC>, "0" digit(s) shall be inserted at the left side to fill the 2 digit coding. If there are less than 4 significant digits in <MMEGI>, "0" digit(s) shall be inserted at the left side to fill the 4 digit coding.

19.4.2.5 Routing Area Identity (RAI) - EPC

The Routing Area Identity (RAI) consists of a RAC, LAC, MNC and MCC.

A subdomain name for use by core network nodes based on RAI shall be derived from the MNC and MCC by adding the label "rac" to the beginning of the Home Network Realm/Domain (see clause 19.2).

The RAI FQDN shall be constructed as:

rac<RAC>.lac<LAC>.rac.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

<RAC> and <LAC> shall be Hex coded digits representing the LAC and RAC codes respectively.

If there are less than 4 significant digits in <RAC> or <LAC>, one or more "0" digit(s) is/are inserted at the left side to fill the 4 digit coding.

Note: Above subdomain is for release 8 core network nodes to allow DNS records other than A/AAAA records. The subdomain name in Annex C.2 are still used for existing A/AAAA records for pre-Release 8 nodes and are also still used for backward compatibility.

19.4.2.6 Serving GPRS Support Node (SGSN) within SGSN pool

A specific SGSN within an operator's network is identified using the RAI FQDN (clause 19.4.2.5) and the Network Resource Identifier (NRI) (see 3GPP TS 23.236 [23]). Such an identifier can be used by a target MME or SGSN node to connect to the source SGSN node.

The SGSN FQDN shall be constructed as:

nri-sgsn<NRI>.rac<RAC>.lac<LAC>.rac.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

<NRI> shall be Hex coded digits representing the NRI code of the SGSN.

If there are less than 4 significant digits in < NRI>, one or more "0" digit(s) is/are inserted at the left side to fill the 4 digit coding. Coding for other fields is the same as in Clause 19.4.2.5.

When a target MME constructs the FQDN of the source SGSN in the case of SGSN pooling, it should derive the NRI from the 8-bit MME Code received in the GUTI from the UE. However, if the length of the NRI, e.g., X, which is configured in the MME is less than 8 bits, then the MME should use only the most significant X bits of the MME Code as the NRI within the SGSN FQDN.

Note: Above subdomain is for release 8 core network nodes to allow DNS records other than A/AAAA records. The subdomain name in Annex C.2 are still used for existing A/AAAA records for pre-Release 8 nodes and are also still used for backward compatibility. .

19.4.2.7 Target RNC-ID for U-TRAN

In the special case of a UTRAN target RNC a possible SGSN that can control that RNC can be identified by RNC-ID. This identifier can be used for SRNS relocation with a U-TRAN target RNC.

A subdomain name for use by core network nodes based on RNC-ID shall be derived from the MNC and MCC by adding the label "rnc" to the beginning of the Home Network Realm/Domain (see clause 19.2).

The RNC FQDN shall be constructed as:

rnc<RNC>.rnc.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

<RNC> shall be Hex coded digits representing the RNC-ID code of the RNC.

If there are less than 4 significant digits in <RNC>, one or more "0" digit(s) is/are inserted at the left side to fill the 4 digit coding.

NOTE: Above subdomain is for release 8 core network nodes to allow DNS records other than A/AAAA records. The subdomain name in Annex C.3 are still used for existing A/AAAA records for pre-Release 8 nodes and are still used for backward compatibility. However, RNC-ID in Annex C.3 was originally intended for the case where only one SGSN controlled an RNC-ID and gave the SGSN IP address. The usage for the above RNC FQDN is potentially broader and can target an SGSN pool.

19.4.2.8 DNS subdomain for operator usage in EPC

The EPC nodes DNS subdomain (DNS zone) shall be derived from the MNC and MCC by adding the label "node" to the beginning of the Home Network Realm/Domain (see clause 19.2) and shall be constructed as:

node.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

This DNS subdomain is formally placed into the operator's control. 3GPP shall never take this DNS subdomain back or any zone cut/subdomain within it for any purpose. As a result the operator can safely provision any DNS records it chooses under this subdomain without concern about future 3GPP standards encroaching on the DNS names within this zone.

19.4.2.9 ePDG FQDN and Visited Country FQDN for non-emergency bearer services

19.4.2.9.1 General

The ePDG Fully Qualified Domain Name (ePDG FQDN), for non-emergency bearers services, shall be constructed using one of the following formats, as specified in clause 4.5.4 of 3GPP TS 23.402 [68]:

- Operator Identifier based ePDG FQDN;
- Tracking/Location Area Identity based ePDG FQDN;
- the ePDG FQDN configured in the UE by the HPLMN.

NOTE: The ePDG FQDN configured in the UE can have a different format than those specified in the following clauses.

The Visited Country FQDN is used by a roaming UE to determine whether the visited country mandates the selection of an ePDG in this country (see clause 4.5.4.5 of 3GPP TS 23.402 [68]). The Visited Country FQDN shall be constructed as specified in clause 19.4.2.9.4. The Replacement field used in DNS-based Discovery of regulatory requirements shall be constructed as specified in clause 19.4.2.9.5.

19.4.2.9.2 Operator Identifier based ePDG FQDN

The ePDG Fully Qualified Domain Name (ePDG FQDN) contains an Operator Identifier that shall uniquely identify the PLMN where the ePDG is located. The ePDG FQDN is composed of seven labels. The last three labels shall be "pub.3gppnetwork.org". The third and fourth labels together shall uniquely identify the PLMN. The first two labels shall be "epdg.epc". The result of the ePDG FQDN will be:

"epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org"

In the roaming case, the UE can utilise the services of the VPLMN or the HPLMN (see 3GPP TS 23.402 [68] and 3GPP TS 24.302 [77]). In this case, the Operator Identifier based ePDG FQDN shall be constructed as described above, but using the MNC and MCC of the VPLMN or the HPLMN.

In order to guarantee inter-PLMN DNS translation, the <MNC> and <MCC> coding used in the "epdg.epc. mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org" format of the Operator Identifier based ePDG FQDN shall be:

- <MNC> = 3 digits
- <MCC> = 3 digits

If there are only 2 significant digits in the MNC, one "0" digit shall be inserted at the left side to fill the 3 digits coding of MNC in the ePDG FQDN.

As an example, the Operator Identifier based ePDG FQDN for MCC 345 and MNC 12 is coded in the DNS as:

"epdg.epc.mnc012.mcc345.pub.3gppnetwork.org".

19.4.2.9.3 Tracking/Location Area Identity based ePDG FQDN

The Tracking/Location Area Identity based ePDG FQDN is used to support location based ePDG selection within a PLMN.

There are two Tracking Area Identity based ePDG FQDNs defined: one based on a TAI with a 2 octet TAC and a 5GS one based on a 3 octet TAC.

1) The Tracking Area Identity based ePDG FQDN using a 2 octet TAC and the Location Area Identity based ePDG FQDN shall be constructed respectively as:

   "tac-lb<TAC-low-byte>.tac-hb<TAC-high-byte>.tac.epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org"

   and

   "lac<LAC>.epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org"

where

- the <MNC> and <MCC> shall identify the PLMN where the ePDG is located and shall be encoded as
  - <MNC> = 3 digits
  - <MCC> = 3 digits

  If there are only 2 significant digits in the MNC, one "0" digit shall be inserted at the left side to fill the 3 digits coding of MNC in the ePDG FQDN.
- the <TAC>, together with the <MCC> and <MNC> shall identify the Tracking Area Identity the UE is located in.

  The TAC is a 16-bit integer. The <TAC-high-byte> is the hexadecimal string of the most significant byte in the TAC and the <TAC-low-byte > is the hexadecimal string of the least significant byte. If there are less than 2 significant digits in <TAC-high-byte> or <TAC-low-byte >, "0" digit(s) shall be inserted at the left side to fill the 2 digit coding;
- the <LAC>, together with the <MCC> and <MNC> shall identify the Location Area Identity the UE is located in.

The LAC> shall be hexadecimal coded digits representing the LAC; if there are less than 4 significant digits in <LAC>, one or more "0" digit(s) is/are inserted at the left side to fill the 4 digit coding;

As examples,

- the Tracking Area Identity based ePDG FQDN for the TAC H'0B21, MCC 345 and MNC 12 is coded in the DNS as:

  " tac-lb21.tac-hb0b.tac.epdg.epc.mnc012.mcc345.pub.3gppnetwork.org"

- the Location Area Identity based ePDG FQDN for the LAC H'0B21, MCC 345 and MNC 12 is coded in the DNS as:

  " lac0b21.epdg.epc.mnc012.mcc345.pub.3gppnetwork.org"

2) The 5GS Tracking Area Identity based ePDG FQDN using a 3 octet TAC shall be constructed respectively as:

"tac-lb<TAC-low-byte>.tac-mb<TAC-middle-byte>.tac-hb<TAC-high-byte>.5gstac.
epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org"

where

- the <MNC> and <MCC> shall identify the PLMN where the ePDG is located and shall be encoded as
  - <MNC> = 3 digits
  - <MCC> = 3 digits

  If there are only 2 significant digits in the MNC, one "0" digit shall be inserted at the left side to fill the 3 digits coding of MNC in the ePDG FQDN.

- the <TAC>, together with the <MCC> and <MNC> shall identify the 5GS Tracking Area Identity the UE is located in.

  The 5GS TAC is a 24-bit integer. The <TAC-high-byte> is the hexadecimal string of the most significant byte in the TAC and the <TAC-low-byte > is the hexadecimal string of the least significant byte. If there are less than 2 significant digits in <TAC-low-byte>, <TAC-middle-byte> or <TAC-high-byte >, "0" digit(s) shall be inserted at the left side to fill the 2 digits coding;

As examples,

- the 5GS Tracking Area Identity based ePDG FQDN for the 5GS TAC H'0B1A21, MCC 345 and MNC 12 is coded in the DNS as:

  "tac-lb21.tac-mb1a.tac-hb0b.5gstac.epdg.epc.mnc012.mcc345.pub.3gppnetwork.org"

19.4.2.9.4 Visited Country FQDN

The Visited Country FQDN, used by a roaming UE to determine whether the visited country mandates the selection of an ePDG in this country, shall be constructed as described below.

The Visited Country FQDN shall contain a MCC that uniquely identifies the country in which the UE is located.

The Visited Country FQDN is composed of seven labels. The last three labels shall be "pub.3gppnetwork.org". The fourth label shall be "visited-country". The third label shall uniquely identify the MCC of the visited country. The first and second labels shall be "epdg.epc". The resulting Visited Country FQDN will be:

"epdg.epc.mcc<MCC>.visited-country.pub.3gppnetwork.org"

The <MCC> coding used in this FQDN shall be:

- <MCC> = 3 digits

As an example, the Visited Country FQDN for MCC 345 is coded in the DNS as:

"epdg.epc. mcc345.visited-country.pub.3gppnetwork.org".

19.4.2.9.5 Replacement field used in DNS-based Discovery of regulatory requirements

If the visited country mandates the selection of an ePDG in this country (see clause 4.5.4.5 of 3GPP TS 23.402 [68]), the NAPTR record(s) associated to the Visited Country FQDN shall be provisioned with the replacement field containing the identity of the PLMN(s) in the visited country which may be used for ePDG selection.

The replacement field shall take the form of an Operator Identifier based ePDG FQDN as specified in clause 19.4.2.9.2.

For countries with multiple MCC, the NAPTR records returned by the DNS may contain a different MCC than the MCC indicated in the Visited Country FQDN.

As an example, the NAPTR records associated to the Visited Country FQDN for MCC 345, and for MNC 012, 013 and 014, are provisioned in the DNS as:

```
epdg.epc.mcc345.visited-country.pub.3gppnetwork.org
;    IN NAPTR   order   pref.flag service   regexp   replacement
     IN NAPTR   100  999 ""        ""        ""   epdg.epc.mnc012.mcc345.pub.3gppnetwork.org
     IN NAPTR   100  999 ""        ""        ""   epdg.epc.mnc013.mcc345.pub.3gppnetwork.org
     IN NAPTR   100  999 ""        ""        ""   epdg.epc.mnc014.mcc345.pub.3gppnetwork.org
```

19.4.2.9A ePDG FQDN for emergency bearer services

19.4.2.9A.1 General

The ePDG FQDN used for the selection of an ePDG supporting emergency bearer services shall be constructed using one of the following formats, as specified in clause 4.5.4a of 3GPP TS 23.402 [68] and 3GPP TS 24.302 [77]:

- an Operator Identifier based Emergency ePDG FQDN;
- a Tracking/Location Area Identity based Emergency ePDG FQDN;
- an Emergency ePDG FQDN configured in the UE by the HPLMN, which may have a different format than the one specified in the following clause.

The Visited Country Emergency FQDN is used by a roaming UE, in the context of an emergency session, to determine whether the visited country mandates the selection of an ePDG in this country. The Visited Country Emergency FQDN shall be constructed as specified in clause 19.4.2.9A.4. The Replacement field used in DNS-based Discovery of regulatory requirements shall be constructed as specified in clause 19.4.2.9A.5.

The Visited Country Emergency Numbers FQDN is used by a roaming UE to determine the list of emergency numbers and related emergency service types in the the visited country.

19.4.2.9A.2 Operator Identifier based Emergency ePDG FQDN

The Operator Identifier based Emergency ePDG FQDN shall be constructed as specified for the Operator Identifier based ePDG FQDN in clause 19.4.2.9.2, with the addition of the label "sos" before the labels "epdg.epc". The result of the Emergency ePDG FQDN will be:

"sos.epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org"

As an example, the Operator Identifier based Emergency ePDG FQDN for MCC 345 and MNC 12 is coded in the DNS as:

"sos.epdg.epc.mnc012.mcc345.pub.3gppnetwork.org".

19.4.2.9A.3 Tracking/Location Area Identity based Emergency ePDG FQDN

There are two Tracking Area Identity based Emergency ePDG FQDNs defined: one based on a TAI with a 2 octet TAC and a 5GS one based on a 3 octet TAC.

1) The Tracking Area Identity based Emergency ePDG FQDN using a 2 octet TAC and the Location Area Identity based Emergency ePDG FQDN shall be constructed as specified for the Tracking Area Identity based ePDG

FQDN and the Location Area Identity based ePDG FQDN in clause 19.4.2.9.3, with the addition of the label "sos" before the labels "epdg.epc".

The result of the Tracking Area Identity based Emergency ePDG FQDN and the Location Area Identity based Emergency ePDG FQDN will be:

"tac-lb<TAC-low-byte>.tac-hb<TAC-high-byte>.tac.sos.epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org"

and

"lac<LAC>.sos.epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org"

As examples,

- the Tracking Area Identity based Emergency ePDG FQDN for the TAC H'0B21, MCC 345 and MNC 12 is coded in the DNS as:

  " tac-lb21.tac-hb0b.tac.sos.epdg.epc.mnc012.mcc345.pub.3gppnetwork.org"

- the Location Area Identity based Emergency ePDG FQDN for the LAC H'0B21, MCC 345 and MNC 12 is coded in the DNS as:

  " lac0b21.sos.epdg.epc.mnc012.mcc345.pub.3gppnetwork.org"

2) The 5GS Tracking Area Identity based Emergency ePDG FQDN using a 3 octet TAC shall be constructed as specified for the 5GS Tracking Area Identity based ePDG FQDN in clause 19.4.2.9.3, with the addition of the label "sos" before the labels "epdg.epc".

The result of the 5GS Tracking Area Identity based Emergency ePDG FQDN will be:

"tac-lb<TAC-low-byte>.tac-mb<TAC-middle-byte>.tac-hb<TAC-high-byte>.5gstac.sos.epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org "

As examples,

- the 5GS Tracking Area Identity based Emergency ePDG FQDN for the 5GS TAC H'0B1A21, MCC 345 and MNC 12 is coded in the DNS as:

  "tac-lb21.tac-mb1a.tac-hb0b.5gstac.sos.epdg.epc.mnc012.mcc345.pub.3gppnetwork.org"

19.4.2.9A.4 Visited Country Emergency FQDN

The Visited Country Emergency FQDN shall be constructed as specified for the Visited Country FQDN in clause 19.4.2.9.4, with the addition of the label "sos" before the labels "epdg.epc".

The result of the Visited Country Emergency FQDN will be:

"sos.epdg.epc.mcc<MCC>.visited-country.pub.3gppnetwork.org"

As an example, the Visited Country Emergency FQDN for MCC 345 is coded in the DNS as:

"sos.epdg.epc. mcc345.visited-country.pub.3gppnetwork.org".

19.4.2.9A.5 Replacement field used in DNS-based Discovery of regulatory requirements for emergency services

The requirements specified in clause 19.4.2.9.5 for the Replacement field used in DNS-based Discovery of regulatory requirements shall apply with the following modification.

The replacement field shall take the form of an Operator Identifier based Emergency ePDG FQDN as specified in clause 19.4.2.9A.2.

As an example, the NAPTR records associated to the Visited Country FQDN for MCC 345, and for MNC 012, 013 and 014, are provisioned in the DNS as:

```
sos.epdg.epc.mcc345.visited-country.pub.3gppnetwork.org
;     IN NAPTR    order     pref.flag service    regexp    replacement
      IN NAPTR    100  999  ""        ""    sos.epdg.epc.mnc012.mcc345.pub.3gppnetwork.org
      IN NAPTR    100  999  ""        ""    sos.epdg.epc.mnc013.mcc345.pub.3gppnetwork.org
      IN NAPTR    100  999  ""        ""    sos.epdg.epc.mnc014.mcc345.pub.3gppnetwork.org
```

19.4.2.9A.6 Country based Emergency Numbers FQDN

The Country based Emergency Numbers FQDN shall be constructed as specified for the Visited Country Emergency FQDN in clause 19.4.2.9A.4, but with replacing the label "epdg" by the label "en".

The result of the Country based Emergency Numbers FQDN will be:

"sos.en.epc.mcc<MCC>.visited-country.pub.3gppnetwork.org"

NOTE: Even though a label named "visited-country" is present, operators in the home country can use the same mechanism to provide emergency numbers and associated type(s).

As an example, the Country based Emergency Numbers FQDN for MCC 345 is coded in the DNS as:

"sos.en.epc. mcc345.visited-country.pub.3gppnetwork.org".

19.4.2.9A.7 Replacement field used in DNS-based Discovery of Emergency Numbers

The NAPTR record(s) associated to the Country based Emergency Numbers FQDN shall be provisioned with the replacement field containing the emergency numbers and related emergency service types.

The replacement field shall take the following form and include both an emergency number and at least one emergency service type:

<emergency-type>.<emergency-number>.sos.en.epc.mcc<MCC>.visited-country.pub.3gppnetwork.org

The <emergency-number> and <emergency-type> shall follow the syntax defined in Table 19.4.2.9A.7-1. The <emergency-number> shall consist of a single label. The <emergency-type> shall consist of at least one label.

Table 19.4.2.9A.7-1: Syntax of emergency number and emergency type

```
emergency-number    = DIGIT*DIGIT                ; at least one DIGIT
emergency-type      = "sos" *("." sub-label)
sub-label           = let-dig [ *61let-dig-hyp let-dig ]
let-dig-hyp         = let-dig / "-"
let-dig         = ALPHA / DIGIT
ALPHA           = %x41-5A / %x61-7A         ; A-Z / a-z
```

As an example, the NAPTR records associated to the Country based Emergency Numbers FQDN for MCC 345 are provisioned in the DNS as:

```
sos.en.epc.mcc345.visited-country.pub.3gppnetwork.org
;     IN NAPTR    order     pref.flag service    regexp    replacement
      IN NAPTR    100  999  ""        ""    sos.ambulance.15.sos.en.epc.mcc345.visited-country.pub.3gppnetwork.org
      IN NAPTR    100  999  ""        ""    sos.police.17.sos.en.epc.mcc345.visited-country.pub.3gppnetwork.org
      IN NAPTR    100  999  ""        ""    sos.fire.18.sos.en.epc.mcc345.visited-country.pub.3gppnetwork.org
        IN NAPTR    100    999    ""      ""  sos.marine.196.sos.en.epc.mcc345.visited-country.pub.3gppnetwork.org
```

19.4.2.10 Global eNodeB-ID for eNodeB

The Global eNodeB-ID is used to identify eNodeBs globally which is composed of the concatenation of MCC, MNC and the eNodeBID. The MCC and MNC are the same as included in the E-UTRAN Cell Global Identifier (ECGI) (see clause 19.6).

A subdomain name shall be derived from the MNC and MCC by adding the label "enb" to the beginning of the Home Network Realm/Domain (see clause 19.2).

The Global eNodeB-ID FQDN shall be constructed as:

enb<eNodeB-ID>.enb.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

The <eNodeB-ID> shall be coded using a full hexadecimal representation. If there are less than 4 significant digits in <eNodeB-ID>, "0" digit(s) shall be inserted at the left side to fill the 4 digit coding.

19.4.2.11 Local Home Network identifier

The Local Home Network identifier uniquely identifies a local home network. For the definition of a local home network see 3GPP TS 23.060 [3] and 3GPP TS 23.401 [72].

A subdomain name shall be derived from the MNC and MCC from the visited network by adding the label "lhn" to the beginning of the Home Network Realm/Domain (see clause 19.2).

The Local Home Network-ID FQDN shall be constructed as:

lhn< LHN name >.lhn.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

The <LHN-name> length and content is an operator choice. The labels shall follow the rules specified in clause 19.4.2.1.

19.4.3 Service and Protocol service names for 3GPP

A list of standardized "service-parms" names is required to identify a "service" as defined in section 6.5 of IETF RFC 3958 [74].

The following table defines the names to be used in the procedures specified in 3GPP TS 29.303 [73]:

Table 19.4.3.1: List of 'app-service' and 'app-protocol' names

Description	IETF RFC 3958 section 6.5 'app-service' name	IETF RFC 3958 section 6.5 'app-protocol' name
PGW and interface types supported by the PGW	x-3gpp-pgw	x-s5-gtp, x-s5-pmip, x-s8-gtp , x-s8-pmip, x-s2a-pmip, x-s2a-mipv4, x-s2a-gtp, x-s2b-pmip, x-s2b-gtp, x-s2c-dsmip, x-gn, x-gp See NOTE.
SGW and interface types supported by the SGW	x-3gpp-sgw	x-s5-gtp, x-s5-pmip, x-s8-gtp, x-s8-pmip, x-s11, x-s12, x-s4, x-s1-u, x-s2a-pmip, x-s2b-pmip See NOTE.
GGSN	x-3gpp-ggsn	x-gn, x-gp See NOTE.
SGSN	x-3gpp-sgsn	x-gn, x-gp, x-s4, x-s3, x-s16, x-sv, x-nqprime See NOTE.
MME and interface types supported by the MME	x-3gpp-mme	x-s10, x-s11, x-s3, x-s6a, x-s1-mme, x-gn, x-gp, x-sv, x-nq See NOTE.
MSC Server	x-3gpp-msc	x-sv
UP function	x-3gpp-upf	x-sxa, x-sxb, x-sxc, x-n4 See NOTE.
AMF	x-3gpp-amf	x-n2 x-n26
NOTE: When using Dedicated Core Networks, the character string "+ue-<ue usage type>" shall be appended to the 'app-protocol' name, for the interfaces applicable to Dedicated Core Networks, where <ue-usage-type>" contains one or more UE usage type values. See 3GPP TS 29.303 [73], 3GPP TS 29.272 [108] and 3GPP TS 29.273 [78]. Example: x-s5-gtp+ue-<ue usage type> If multiple UE usage type values are embedded in the "+ue-<ue usage type>", they shall be separated by the symbol ".", e.g. "+ue-1.3.4.20" as specified in IETF RFC 3958 [74]. To select a network node with a particular network capability needed, the character string "+nc-<network capability>" shall be appended to the 'app-protocol' name, where < network capability > contains one or more network capability of the node. See 3GPP TS 29.303 [73]. Example: x-s5-gtp+nc-<network capability> If multiple network capability of the node are embedded in the "+nc-<network capability>", they shall be separated by the symbol ".", e.g. "+nc-nr.smf", as specified in IETF RFC 3958 [74]. To select a network node with a particular network capability needed within a certain Dedicated Core Networks, the character string "+nc-<network capability>" and "+ue-<ue usage type>" shall be appended to the 'app-protocol' name, where <ue usage type> contains one or more UE usage type values and the Example: x-s5-gtp+nc-<network capability>+ue-<ue usage type> or x-s5-gtp+ue-<ue usage type>+nc-<network capability>		

NOTE 1: The formats follow the experimental format as specified in IETF RFC 3958 [74]. For example, to find the S8 PMIP interfaces on a PGW the Service Parameter of "3gpp-pgw:x-s8-pmip" would be used as input in the procedures defined in IETF RFC 3958 [74].

NOTE 2: Currently 'app-service' names identify 3GPP node type and 'app-protocol' identify 3GPP interfaces, which differs from more common usage of S-NAPTR where app-protocol is used for transport protocol. Type of nodes (i.e PGW, SGW, SGSN, MME, MSC Server etc) and interfaces (i.e. S11, S5, S8, Sv, etc.) follow the standard names from 3GPP TS 23.401 [72] ,3GPP TS 29.060 [6] and3GPP TS 23.216 [92] with prefix "x-" added.

NOTE 3: x-gn denotes an intra-PLMN interface using GTPv1-C, x-gp denotes an inter-PLMN interface using GTPv1-C.

NOTE 4: The app-service of x-3gpp-pgw with app-protocols x-gn or x-gp identifies the co-located GGSN function on a PGW. The app-service of x-3gpp-ggsn with app-protocols x-gn or x-gp identifies a GGSN function that is not co-located with a PGW.

NOTE 5: The app-service of x-3gpp-msc with app-protocol x-sv identifies the MSC Sv interface service.

NOTE 6: The app-service of x-3gpp-amf with app-protocol x-n2 identifies the AMF N2 interface service. The app-service of x-3gpp-amf with app-protocol x-n26 identifies the AMF N26 interface service.

19.5 Access Network Identity

A trusted non-3GPP access network used by the UE to access EPS can be identified using the Access Network Identity. The Access Network Identity is used as an input parameter in the EPS security procedures as specified in 3GPP TS 33.402 [69]. The format and signalling of the parameter between the network and the UE is specified in 3GPP TS 24.302 [77] and the format and signalling of this parameter between access network and core network is specified in 3GPP TS 29.273 [78].

The encoding of the Access Network Identity shall be specified within 3GPP, but the Access Network Identity definition for each non-3GPP access network is under the responsibility of the corresponding standardisation organisation respectively.

19.6 E-UTRAN Cell Identity (ECI) and E-UTRAN Cell Global Identification (ECGI)

The E-UTRAN Cell Global Identification (ECGI) shall be composed of the concatenation of the PLMN Identifier (PLMN-Id) and the E-UTRAN Cell Identity (ECI) as shown in figure 19.6.1 and shall be globally unique:

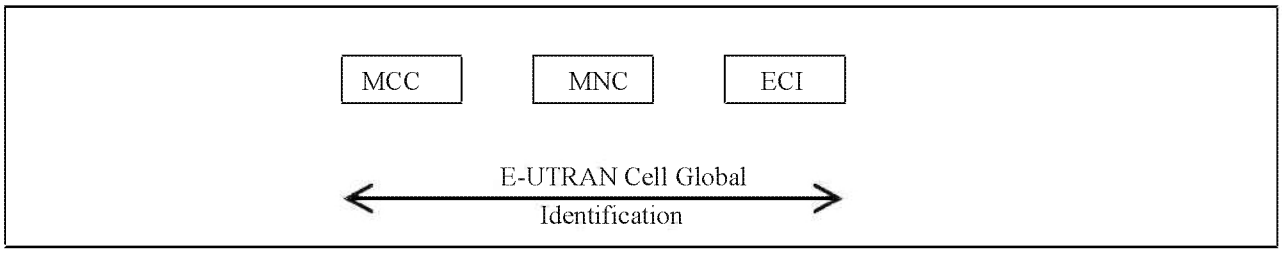

Figure 19.6.1: Structure of E-UTRAN Cell Global Identification

The ECI shall be of fixed length of 28 bits and shall be coded using full hexadecimal representation. The exact coding of the ECI is the responsibility of each PLMN operator.

For more details on ECI and ECGI, see 3GPP TS 36.413 [84].

19.6A NR Cell Identity (NCI) and NR Cell Global Identity (NCGI)

The NR Cell Global Identity (NCGI) shall be composed of the concatenation of the PLMN Identifier (PLMN-Id) and the NR Cell Identity (NCI) as shown in figure 19.6A-1 and shall be globally unique:

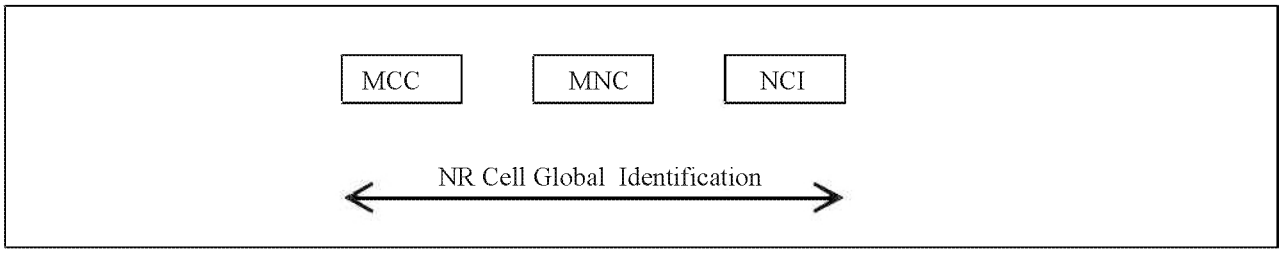

Figure 19.6A-1: Structure of NR Cell Global Identity

The NCI shall be of fixed length of 36 bits and shall be coded using full hexadecimal representation. The exact coding of the NCI is the responsibility of each PLMN operator.

For more details on NCI and NCGI, see 3GPP TS 38.413 [123].

19.7 Identifiers for communications with packet data networks and applications

19.7.1 Introduction

This clause describes external identifiers used to facilitate communications with packet data networks and applications (e.g. Machine Type Communication (MTC) applications on the external network/MTC servers) as specified in 3GPP TS 23.682 [98], 3GPP TS 23.501 [119] and 3GPP TS 23.502 [120].

19.7.2 External Identifier

An External Identifier identifies a subscription associated to an IMSI. A subscription associated to an IMSI may have one or several External Identifier(s).

The External Identifier shall have the form username@realm as specified in clause 2.1 of IETF RFC 4282 [53].

The username part format of the External Identifier shall contain a Local Identifier as specified in 3GPP TS 23.682 [98]. The realm part format of the External Identifier shall contain a Domain Identifier as specified in 3GPP TS 23.682 [98]. As specified in clause 4 of IETF RFC 4282 [53], the Domain Identifier shall be a duly registered Internet domain name. The combination of Local Identifier and Domain Identifier makes the External Identifier globally unique.

The result of the External Identifier form is:

"<Local Identifier>@<Domain Identifier>"

An example of an External Identifier is:

Local Identifier in use: "123456789";

Domain Identifier = "domain.com";

Which gives the External Identifier as:

123456789@domain.com

19.7.3 External Group Identifier

An External Group Identifier identifies a group made up of one or more subscriptions associated to a group of IMSIs.

The External Group Identifier shall have the form groupname@realm as specified in clause 2.1 of IETF RFC 4282 [53].

The groupname part format of the External Group Identifier shall contain a Local Identifier as specified in 3GPP TS 23.682 [98]. The realm part format of the External Group Identifier shall contain a Domain Identifier as specified in 3GPP TS 23.682 [98]. As specified in clause 4 of IETF RFC 4282 [53], the Domain Identifier shall be a duly registered Internet domain name. The combination of Local Identifier and Domain Identifier makes the External Group Identifier globally unique.

The result of the External Group Identifier form is:

"<Local Identifier>@<Domain Identifier>"

An example of an External Group Identifier is:

Local Identifier in use: "Group1";

Domain Identifier = "domain.com";

Which gives the External Group Identifier as:

Group1@domain.com

19.8 TWAN Operator Name

The TWAN Operator Name identifies the TWAN operator when the TWAN is not operated by a mobile operator.

The TWAN Operator Name shall be encoded as a realm in the form of an Internet domain name, e.g. operator.com, as specified in IETF RFC 1035 [19] and IETF RFC 1123 [20]. The TWAN Operator Name consists of one or more labels. Each label shall consist of the alphabetic characters (A-Z and a-z), digits (0-9) and the hyphen (-) in accordance with IETF RFC 1035 [19]. Each label shall begin and end with either an alphabetic character or a digit in accordance with IETF RFC 1123 [20]. The case of alphabetic characters is not significant.

NOTE: The TWAN Operator Name is encoded as a dotted string.

19.9 IMSI-Group Identifier

IMSI-Group Identifier is a network internal globally unique ID which identifies a set of IMSIs (e.g. MTC devices) from a given network that are grouped together for one specific group related services. It is used e.g. for group specifc NAS level congestion control (see 3GPP TS 23.401 [72]).

An IMSI-Group Identifier shall be composed as shown in figure 19.9-1.

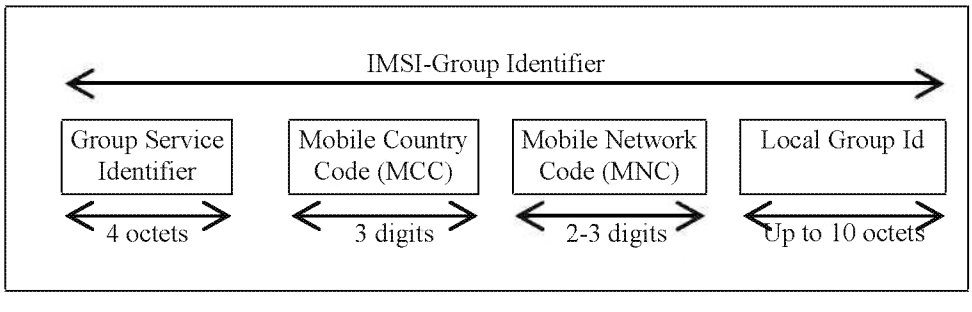

Figure 19.9-1: Structure of IMSI-Group Identifier

IMSI-Group Identifier is composed of four parts:

1) Group Service Identifier, identifies the service (4 Octets) for which the IMSI-Group Identifier is valid.

2) Mobile Country Code (MCC) consisting of three digits. The MCC identifies uniquely the country of domicile of the mobile subscriber;

3) Mobile Network Code (MNC) consisting of two or three digits. The MNC identifies the home PLMN of the mobile subscriber. The length of the MNC (two or three digits) depends on the value of the MCC. A mixture of two and three digit MNC codes within a single MCC area is not recommended and is outside the scope of this specification.

4) the Local Group Id is assigned by the network operator and may have a length of up to 10 octets.

Two different IMSI-Group Identifier values, with the same Group Service Identifier and with MCC/MNC values that point to the same PLMN, shall have two different Local Group Ids.

19.10 Presence Reporting Area Identifier (PRA ID)

The Presence Reporting Area Identifier (PRA ID) is used to identify a Presence Reporting Area (PRA).

PRAs can be used for reporting changes of UE presence in a PRA, e.g. for policy control or charging decisions. See 3GPP TS 23.401 [72], 3GPP TS 23.060 [3] and 3GPP TS 23.203 [107].

A PRA is composed of a short list of TAs/RAs, or eNBs and/or cells/SAs in a PLMN. A PRA can be:

- either a "UE-dedicated PRA", defined in the subscriber profile;
- or a "Core Network predefined PRA", pre-configured in MME/S4-SGSN.

PRA IDs used to identify "Core Network predefined PRAs" shall not be used for identifying "UE-dedicated PRAs".

The same PRA ID may be used for different UEs to identify different "UE-dedicated PRAs", i.e. PRA IDs may overlap between different UEs, while identifying different "UE-dedicated PRAs".

The PRA ID shall be encoded as an integer on 3 octets. The most significant bit of the PRA ID shall be set to 0 for UE-dedicated PRA and shall be to 1 for Core Network predefined PRA.

19.11 Dedicated Core Networks Identifier

A Dedicated Core Network ID (DCN-ID) identifies a Dedicated Core Network (DCN) within a PLMN.

The allowed values of DCN-ID shall be in the range of 0 to 65535.

Values in the range of 0 to 127 are standardized and defined as follows:

0: Spare, for future use

…

127: Spare, for future use

Values in the range of 128 to 65535 are operator-specific.

The use of the standardized DCN-ID is specified in 3GPP TS 23.401 [72].

20 Addressing and Identification for IMS Centralized Services

20.1 Introduction

This clause describes the format of the parameters needed specifically for IMS Centralized Services (ICS). For further information on the use of ICS parameters, see 3GPP TS 23.292 [70].

20.2 UE based solution

In this solution, the UE is provisioned with an ICS specific client that simply reuses IMS registration as defined in 3GPP TS 23.228 [24]. Therefore, ICS capable UE shall reuse the identities defined in clause 13.

20.3 Network based solution

20.3.1 General

In this solution the MSC Server enhanced for ICS performs a special IMS registration on behalf of the UE. Thus, the MSC Server enhanced for ICS shall use a Private User Identity and Temporary Public User Identity that are different to those defined in clause 13 (see 3GPP TS 23.292 [70], clause 4.6.2 for more information). Furthermore, the MSC Server enhanced for ICS derives a Conference Factory URI that is known to the home IMS. These are defined in the following clauses.

20.3.2 Home network domain name

The home network domain name shall be in the form of an Internet domain name, e.g. operator.com, as specified in IETF RFC 1035 [19] and IETF RFC 1123 [20]. The home network domain name consists of one or more labels. Each label shall consist of the alphabetic characters (A-Z and a-z), digits (0-9) and the hyphen (-) in accordance with IETF RFC 1035 [19]. Each label shall begin and end with either an alphabetic character or a digit in accordance with IETF RFC 1123 [20]. The case of alphabetic characters is not significant.

The MSC Server enhanced for ICS shall derive the home network domain name from the subscriber's IMSI as described in the following steps:

1. Take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used (see 3GPP TS 31.102 [27]) and separate them into MCC and MNC; if the MNC is 2 digits then a zero shall be added at the beginning.
2. Use the MCC and MNC derived in step 1 to create the "mnc<MNC>.mcc<MCC>.3gppnetwork.org" domain name.
3. Add the label "ics." to the beginning of the domain.

An example of a home network domain name is:

IMSI in use: 234150999999999;

where:

- MCC = 234;
- MNC = 15; and
- MSIN = 0999999999,

which gives the home network domain name: ics.mnc015.mcc234.3gppnetwork.org

20.3.3 Private User Identity

The Private User Identity shall take the form of an NAI, and shall have the form "username@realm" as specified in clause 2.1 of IETF RFC 4282 [53].

The MSC Server enhanced for ICS shall derive the Private User Identity from the subscriber's IMSI as follows:

1. Use the whole string of digits as the username part of the private user identity; and
2. convert the leading digits of the IMSI, i.e. MNC and MCC, into a domain name, as described in clause 20.3.2.

The result will be a Private User Identity of the form "<IMSI>@ics.mnc<MNC>.mcc<MCC>.3gppnetwork.org". For example if the IMSI is 234150999999999 (MCC = 234, MNC = 15), the private user identity then takes the form 234150999999999@ics.mnc015.mcc234.3gppnetwork.org

20.3.4 Public User Identity

The Public User Identity shall take the form of a SIP URI (see IETF RFC 3261 [26]), and shall have the form "sip:username@domain".

The MSC Server enhanced for ICS shall derive the Public User Identity from the subscriber's IMSI. The Public User Identity shall consist of the string "sip:" appended with a username and domain portion equal to the IMSI derived Private User Identity described in clause 20.3.3. An example using the same example IMSI from clause 20.3.3 can be found below:

EXAMPLE: "sip:234150999999999@ics.mnc015.mcc234.3gppnetwork.org".

20.3.5 Conference Factory URI

The Conference Factory URI shall take the form of a SIP URI (see IETF RFC 3261 [26]) with a host portion set to the home network domain name as described in clause 20.3.2 prefixed with "conf-factory.". An example using the same example IMSI from clause 20.3.2 can be found below:

EXAMPLE: "sip:conf-factory.ics.mnc015.mcc234.3gppnetwork.org".

The user portion of the SIP URI is optional and implementation specific.

21 Addressing and Identification for Dual Stack Mobile IPv6 (DSMIPv6)

21.1 Introduction

This clause describes the format of the parameters needed by the UE to use Dual Stack Mobile IPv6 (DSMIPv6 as specified in 3GPP TS 23.327 [76] and 3GPP TS 23.402 [68].

21.2 Home Agent – Access Point Name (HA-APN)

21.2.1 General

The HA-APN is composed of two parts as follows:

- The HA-APN Network Identifier; this defines to which external network the HA is connected.
- The HA-APN Operator Identifier; this defines in which PLMN the HA serving the HA-APN is located.

The HA-APN Operator Identifier is placed after the HA-APN Network Identifier. The HA-APN consisting of both the Network Identifier and Operator Identifier corresponds to a FQDN of a HA; the HA-APN has, after encoding as defined in the paragraph below, a maximum length of 100 octets.

The encoding of the HA-APN shall follow the Name Syntax defined in IETF RFC 2181 [18], IETF RFC 1035 [19] and IETF RFC 1123 [20]. The HA-APN consists of one or more labels. Each label is coded as a one octet length field followed by that number of octets coded as 8 bit ASCII characters. Following IETF RFC 1035 [19] the labels shall consist only of the alphabetic characters (A-Z and a-z), digits (0-9) and the hyphen (-). Following IETF RFC 1123 [20], the label shall begin and end with either an alphabetic character or a digit. The case of alphabetic characters is not significant. The HA-APN is not terminated by a length byte of zero.

For the purpose of presentation, a HA-APN is usually displayed as a string in which the labels are separated by dots (e.g. "Label1.Label2.Label3").

21.2.2 Format of HA-APN Network Identifier

The HA-APN Network Identifier follows the format defined for APNs in clause 9.1.1. In addition to what has been defined in clause 9.1.1 the HA-APN Network Identifier shall not contain "ha-apn." or "w-apn." and not end in ".3gppnetwork.org".

A HA-APN Network Identifier may be used to access a service associated with a HA. This may be achieved by defining:

- a HA-APN which corresponds to a FQDN of a HA, and which is locally interpreted by the HA as a request for a specific service, or
- a HA-APN Network Identifier consisting of 3 or more labels and starting with a Reserved Service Label, or a HA-APN Network Identifier consisting of a Reserved Service Label alone, which indicates a HA by the nature of the requested service. Reserved Service Labels and the corresponding services they stand for shall be agreed between operators who have roaming agreements.

As an example, the HA-APN for MCC 345 and MNC 12 is coded in the DNS as:

"internet.ha-apn.mnc012.mcc345.pub.3gppnetwork.org".

where "internet" is the HA-APN Network Identifier and "mnc012.mcc345.pub.3gppnetwork.org " is the HA-APN Operator Identifier.

21.2.3 Format of HA-APN Operator Identifier

The HA-APN Operator Identifier is composed of six labels. The last three labels shall be "pub.3gppnetwork.org". The second and third labels together shall uniquely identify the PLMN. The first label distinguishes the domain name as a HA-APN.

For each operator, there is a default HA-APN Operator Identifier (i.e. domain name). This default HA-APN Operator Identifier is derived from the IMSI as follows:

"ha-apn.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org"

where:

"mnc" and "mcc" serve as invariable identifiers for the following digits.

<MNC> and <MCC> are derived from the components of the IMSI defined in clause 2.2.

Alternatively, the default HA-APN Operator Identifier is derived using the MNC and MCC of the VPLMN.

In order to guarantee inter-PLMN DNS translation, the <MNC> and <MCC> coding used in the "ha-apn.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org" format of the HA-APN OI shall be:

- <MNC> = 3 digits
- <MCC> = 3 digits

If there are only 2 significant digits in the MNC, one "0" digit shall be inserted at the left side to fill the 3 digits coding of MNC in the HA-APN OI.

As an example, the HA-APN OI for MCC 345 and MNC 12 is coded in the DNS as:

"ha-apn.mnc012.mcc345.pub.3gppnetwork.org".

22 Addressing and identification for ANDSF

22.1 Introduction

This clause describes the format of the parameters needed by the UE to use Access Network Discovery and Selection Function (ANDSF) as specified in 3GPP TS 23.402 [68].

22.2 ANDSF Server Name (ANDSF-SN)

22.2.1 General

ANDSF Server Name (ANDSF-SN) is used by UE to discover ANDSF Server in the network.

22.2.2 Format of ANDSF-SN

The ANDSF-SN is composed of six labels. The last three labels shall be "pub.3gppnetwork.org". The second and third labels together shall uniquely identify the PLMN. The first label shall be "andsf".

The ANDSF-SN is derived from the IMSI or Visited PLMN Identity as follows:

"andsf.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org"

where:

"mnc" and "mcc" serve as invariable identifiers for the following digits.

- When contacting Visited ANDSF (V-ANDSF), the <MNC> and <MCC> shall be derived from the Visited PLMN Identity as defined in clause 12.1.

- When contacting Home ANDSF (H-ANDSF), the <MNC> and <MCC> shall be derived from the components of the IMSI defined in clause 2.2.

In order to guarantee inter-PLMN DNS translation, the <MNC> and <MCC> coding used in the "andsf.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org" format of the ANDSF-SN shall be:

- <MNC> = 3 digits
- <MCC> = 3 digits

If there are only 2 significant digits in the MNC, one "0" digit shall be inserted at the left side to fill the 3 digits coding of MNC in the ANDSF-SN.

As an example, the ANDSF-SN OI for MCC 345 and MNC 12 is coded in the DNS as:

"andsf.mnc012.mcc345.pub.3gppnetwork.org".

23 Numbering, addressing and identification for the OAM System

23.1 Introduction

This clause describes some information needed to access the OAM system as specified in TS 36.300 [91]. For more information on the ".3gppnetwork.org" domain name and its applicability, see Annex D of the present document.

23.2 OAM System Realm/Domain

The OAM System Realm/Domain shall be in the form of an Internet domain name, e.g. operator.com, as specified in IETF RFC 1035 [19] and IETF RFC 1123 [20]. The OAM System Realm/Domain consists of one or more labels. Each label shall consist of the alphabetic characters (A-Z and a-z), digits (0-9) and the hyphen (-) in accordance with IETF RFC 1035 [19]. Each label shall begin and end with either an alphabetic character or a digit in accordance with IETF RFC 1123 [20]. The case of alphabetic characters is not significant.

The OAM System Realm/Domain shall be in the form of "oam.mnc<MNC>.mcc<MCC>.3gppnetwork.org", where "<MNC>" and "<MCC>" fields correspond to the MNC and MCC of the operator's PLMN. Both the "<MNC>" and "<MCC>" fields are 3 digits long. If the MNC of the PLMN is 2 digits, then a zero shall be added at the beginning.

For example, the OAM System Realm/Domain of an IMSI shall be derived as described in the following steps:

1. take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used (see 3GPP TS 31.102 [27]) and separate them into MCC and MNC; if the MNC is 2 digits then a zero shall be added at the beginning;
2. use the MCC and MNC derived in step 1 to create the "mnc<MNC>.mcc<MCC>.3gppnetwork.org" domain name;
3. add the label "oam" to the beginning of the domain name.

An example of an OAM System Realm/Domain is:

IMSI in use: 234150999999999;

Where:

MCC = 234;

MNC = 15;

MSIN = 0999999999;

Which gives the OAM System Realm/Domain name: oam.mnc015.mcc234.3gppnetwork.org.

NOTE: If it is not possible for a Relay Node to identify whether a 2 or 3 digit MNC is used (e.g. USIM is inserted and the length of MNC in the IMSI is not available in the "Administrative data" data file), it is implementation dependent how the Relay Node determines the length of the MNC (2 or 3 digits).

23.3 Identifiers for Domain Name System procedures

23.3.1 Introduction

This clause describes Domain Name System (DNS) related identifiers used by the procedures specified in 3GPP TS 29.303 [73].

23.3.2 Fully Qualified Domain Names (FQDNs)

23.3.2.1 General

See clause 19.4.2.1.

23.3.2.2 Relay Node Vendor-Specific OAM System

As part of the startup procedure, relay nodes (see 3GPP TS 36.300 [91], clause 4.7) needs to discover its Operations and Maintainence (OAM) system. A relay node vendor-specific OAM system within an operator's network is identified using the relay node type allocation code from IMEI or IMEISV (IMEI-TAC), MNC and MCC from IMSI and in some cases also tracking area code information associated to the eNB serving the relay node.

A subdomain name for use by EUTRAN OAM system nodes shall be derived from the MNC and MCC by adding the label "eutran" to the beginning of the OAM System Realm/Domain (see clause 23.2).

The vendor-specific relay node OAM system FQDN shall be constructed as following:

- tac-lb<TAC-low-byte>.tac-hb<TAC-high-byte>.imei-tac<IMEI-TAC>.eutran-rn.oam.mnc<MNC>.mcc<MCC>.3gppnetwork.org

The IMEI-TAC is 8 decimal digits (see clause 6.2).

NOTE: IMEI-TAC is used for the type allocation code from IMEI or IMEISV instead of TAC in this clause in order to separate it from the tracking area code (TAC).

The TAC is a 16 bit integer. <TAC-high-byte> is the hexadecimal string of the most significant byte in the TAC and <TAC-low-byte > is the hexadecimal string of the least significant byte. If there are less than 2 significant digits in <TAC-high-byte> or <TAC-low-byte >, "0" digit(s) shall be inserted at the left side to fill the 2 digit coding.

23.3.2.3 Multi-vendor eNodeB Plug-and Play Vendor-Specific OAM System

23.3.2.3.1 General

This clause describes the Fully Qualified Domain Names (FQDNs) used in Multi Vendor Plug and Connect (MvPnC) procedures (see 3GPP TS 32.508 [102]).

The FQDNs used in MvPnC shall be in the form of an Internet domain name and follow the general encoding rules specified in clause 19.4.2.1.

The format of FQDNs used in MvPnC shall follow the "<vendor ID>.<system>.<OAM realm>" pattern.

NOTE: "<vendor ID>.<system>.oam" represents the <service_id> shown in the first row of table E.1.

The <vendor ID> label is optional and is only used in the operator deployments where multiple instances of a particular network entity type are not provided by the same vendor. If present, the <vendor ID> label shall be in the form "vendor<ViD>", where <ViD> field corresponds to the ID of the vendor.

The format of the ViD is vendor specific.

The details of the <system> label are specified in the clauses below.

23.3.2.3.2 Certification Authority server

The Certification Authority server (CA/RA) FQDN shall be derived as follows. The "cara" <system> label is added in front of the operator's OAM realm domain name:

cara.oam.mnc<MNC>.mcc<MCC>.3gppnetwork.org

If particular operator deployment scenarios where there are multiple CA/RA servers (one per vendor), the <vendor ID> label is added in front of the "cara" label:

vendor<ViD>.cara.oam.mnc<MNC>.mcc<MCC>.3gppnetwork.org

An example of a CA/RA FQDN is:

MCC = 123;

MNC = 45;

ViD = abcd;

which gives the CA/RA FQDN: "cara.oam.mnc045.mcc123.3gppnetwork.org" and "vendorabcd.cara.mnc045.mcc123.3gppnetwork.org".

23.3.2.3.3 Security Gateway

The Security Gateway (SeGW) FQDN shall be derived as follows. The "segw" <system> label is added in front of the operator's OAM realm domain name:

segw.oam.mnc<MNC>.mcc<MCC>.3gppnetwork.org

If particular operator deployment scenarios where there are multiple Security Gateways (one per vendor), the <vendor ID> label is added in front of the "segw" label:

vendor<ViD>.segw.oam.mnc<MNC>.mcc<MCC>.3gppnetwork.org

An example of a SeGW FQDN is:

MCC = 123;

MNC = 45;

ViD = abcd;

which gives the SeGW FQDN: "segw.oam.mnc045.mcc123.3gppnetwork.org" and "vendorabcd.segw.mnc045.mcc123.3gppnetwork.org".

23.3.2.3.4 Element Manager

The Element Manager (EM) FQDN shall be derived as follows. The "em" <system> label is added in front of the operator's OAM realm domain name:

em.oam.mnc<MNC>.mcc<MCC>.3gppnetwork.org

If particular operator deployment scenarios where there are multiple Element Managers (one per vendor), the <vendor ID> label is added in front of the "em" label:

vendor<ViD>.em.oam.mnc<MNC>.mcc<MCC>.3gppnetwork.org

An example of a EM FQDN is:

MCC = 123;

MNC = 45;

ViD = abcd;

which gives the EM FQDN: "em.oam.mnc045.mcc123.3gppnetwork.org" and "vendorabcd.em.mnc045.mcc123.3gppnetwork.org".

24 Numbering, addressing and identification for Proximity-based Services (ProSe)

24.1 Introduction

This clause describes the format of the parameters used for ProSe. For further information on the use of the parameters see 3GPP TS 23.303 [103].

24.2 ProSe Application ID

24.2.1 General

The ProSe Application ID is composed of two parts as follows:

- The ProSe Application ID Name, which is described in its entirety by a data structure characterized by different levels e.g, broad-level business category (Level 0) / business sub-category (Level 1) / business name (Level 2) / shop ID (Level 3).
- The PLMN ID, which corresponds to the PLMN that assigned the ProSe Application ID Name.

The PLMN ID is placed before the ProSe Application ID Name as shown in Figure 24.2.1. The PLMN ID and the ProSe Application ID Name shall be separated by a dot.

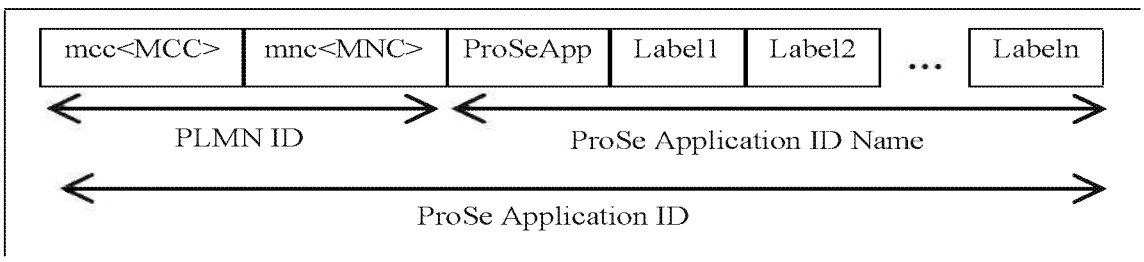

Figure 24.2.1-1: Structure of ProSe Application ID

24.2.2 Format of ProSe Application ID Name in ProSe Application ID

The ProSe Application ID Name is composed of a string of labels. These labels represent hierarchical levels and shall be separated by dots (e.g. "Label1.Label2.Label3"). The ProSe Application ID Name shall contain at least one label. The first label on the left shall be "ProSeApp".

NOTE: The hierarchical structure and the content of the ProSe Application ID Name are outside the scope of 3GPP.

Any label in the ProSe Application ID Name except the first label on the left ("ProSeApp") can be wild carded. A wild card label is represented as "*",

EXAMPLE: A ProSe Application ID Name used to discover nearby Italian restaurants could be "ProSeApp.Food.Restaurants.Italian".

24.2.3 Format of PLMN ID in ProSe Application ID

The PLMN ID shall uniquely identify the PLMN of the ProSe Function that has assigned the ProSe Application ID. The PLMN ID is composed of two labels which shall be separated by a dot as follows:

"mcc<MCC>.mnc<MNC>"

where:

"mcc" and "mnc" serve as invariable identifiers for the following digits.

<MCC> contains the MCC (Mobile Country Code) of the ProSe Function that has assigned the ProSe Application ID.

<MNC> contains the MNC (Mobile Network Code) of the ProSe Function that has assigned the ProSe Application ID.

In order to guarantee inter-PLMN operability, the <MCC> and the <MNC> shall be represented by 3 digits. If there are only 2 significant digits in the MNC, one "0" digit is inserted at the left side of the MNC to form the <MNC> in the "mnc<MNC>" label.

EXAMPLE: The PLMN ID for MCC 345 and MNC 12 will be "mcc345.mnc012".

24.2.4 Usage of wild cards in place of PLMN ID in ProSe Application ID

If the scope of the ProSe Application ID is country-specific, the PLMN ID part in the ProSe Application ID shall be replaced by "mcc<MCC>.mnc*" with <MCC> set to the MCC of the corresponding country.

NOTE: Handling of the case when a country has been allocated more than one MCC value is outside the scope of 3GPP.

If the scope of the ProSe Application ID is global, the PLMN ID part in the ProSe Application ID shall be replaced by "mcc*.mnc*".

EXAMPLE: For a ProSe Application ID specific to a country with MCC 345, the PLMN ID part will be replaced by "mcc345.mnc*".

24.2.5 Informative examples of ProSe Application ID

Examples of ProSe Application IDs following the format defined in the previous clauses are provided for information below.

EXAMPLE 1: "mcc345.mnc012.ProSeApp.Food.Restaurants.Italian"

EXAMPLE 2: "mcc300.mnc165.ProSeApp.Shops.Sports.Surfing"

EXAMPLE 3: "mcc300.mnc165.ProSeApp.*.Sports.Surfing"

EXAMPLE 4: "mcc208.mnc*.ProSeApp.Shops.Food.Wine"

EXAMPLE 5: "mcc*.mnc*.ProSeApp.Food.Restaurants.Coffee"

24.3 ProSe Application Code

24.3.1 General

The ProSe Application Code as described in 3GPP TS 23.303 [103] is composed of the following two parts:

- The PLMN ID of the ProSe Function that assigned the ProSe Application Code, i.e. Mobile Country Code (MCC) and Mobile Network Code (MNC).

- A temporary identity that corresponds to the ProSe Application ID Name. The temporary identity is allocated by the ProSe Function and it may contain a metadata index. The internal structure of the temporary identity is not specified in 3GPP.

The ProSe Application Code shall have a fixed length of 184 bits.

24.3.2 Format of PLMN ID in ProSe Application Code

The PLMN ID in the ProSe Application Code is composed as shown in Figure 24.3.2-1:

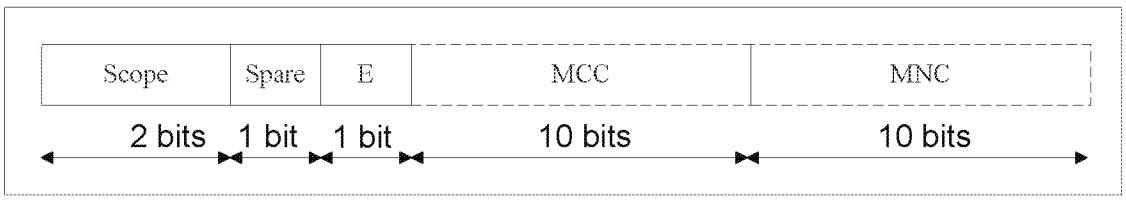

Figure 24.3.2-1: Structure of PLMN ID in ProSe Application Code

The PLMN-ID is composed of four parts:

- Scope indicates whether the MNC, or both the MCC and the MNC, or neither are wild carded in the ProSe Application ID associated with the ProSe Application Code, with the following mapping:

  00 global scope.

  01 reserved.

  10 country-specific scope.

  11 PLMN-specific scope.

- Spare bit that shall be set to 0 and shall be ignored if set to 1.

- E bit indicates whether the MCC and the MNC of the ProSe Function that has assigned the ProSe Application Code are included in the PLMN ID in ProSe Application Code, with the following mapping:

  0 Neither MCC nor MNC is included.

  1 MCC and MNC included.

- When present, the MCC and the MNC shall each have a fixed length of 10 bits and shall be coded as the binary representation of their decimal value.

In this release, the MCC and the MNC of the ProSe Function that has assigned the ProSe Application Code shall always be included in the PLMN ID in ProSe Application Code. The E bit shall always be set to 1.

24.3.3 Format of temporary identity in ProSe Application Code

The temporary identity in the ProSe Application Code is a bit string whose value is allocated by the ProSe Function. The length of the temporary identity in the ProSe Application Code is equal to:

- 180 bits when the E bit of the PLMN ID in the ProSe Application Code is set to 0.

- 160 bits when the E bit of the PLMN ID in the ProSe Application Code is set to 1.

The temporary identity in the ProSe Application Code shall contain a metadata index to reflect the current metadata version if dynamic metadata is used when allocating the ProSe Application Code. The content, position and length of metadata index is operator specific.

In this release, the MCC and the MNC of the ProSe Function that has assigned the ProSe Application Code are always included in the PLMN ID in ProSe Application Code. The length of the temporary identity in the ProSe Application Code shall always be equal to 160 bits.

24.3A ProSe Application Code Prefix

The ProSe Application Code Prefix as described in 3GPP TS 23.303 [103] is to be used with a ProSe Application Code Suffix. The ProSe Application Code Prefix has the same composition and format as the ProSe Application Code, with the following exceptions:

- The temporary identity part of the ProSe Application Code Prefix is of variable length. The length of the temporary identity part shall be incremented in multiple of 8, with a minimum size of 8 bits and a maximum size of 152 bits.
- The sum of the length of the ProSe Application Code Prefix and the length of the ProSe Application Code Suffix shall be 184 bits.

24.3B ProSe Application Code Suffix

The ProSe Application Code Suffix as described in 3GPP TS 23.303 [103] is an identifier to be appended to a ProSe Application Code Prefix. The ProSe Application Code Suffix is of variable length. The length of the ProSe Application Code Suffix shall be incremented in multiple of 8, with a minimum size of 8 bits and a maximum size of 152 bits. The sum of the length of the ProSe Application Code Prefix and the length of the ProSe Application Code Suffix shall be 184 bits.

24.4 EPC ProSe User ID

24.4.1 General

The EPC ProSe User ID as described in 3GPP TS 23.303 [103] identifies the UE registered for EPC-level ProSe Discovery in the context of the ProSe Function.

24.4.2 Format of EPC ProSe User ID

The EPC ProSe User ID is a bit string whose value is allocated by the ProSe Function. The length of the EPC ProSe User ID is equal to 32 bits.

24.5 Home PLMN ProSe Function Address

The Home PLMN ProSe Function address is in the form of a Fully Qualified Domain Name as defined in IETF RFC 1035 [19] and IETF RFC 1123 [20]. This address consists of six labels. Each label shall consist of the alphabetic characters (A-Z and a-z), digits (0-9) and the hyphen (-) in accordance with IETF RFC 1035 [19]. Each label shall begin and end with either an alphabetic character or a digit in accordance with IETF RFC 1123 [20]. The case of alphabetic characters is not significant.

For 3GPP systems, if not pre-configured on the UE or provisioned by the network, the UE shall derive the Home PLMN ProSe Function address from the IMSI as described in the following steps:

1. Take the first 5 or 6 digits, depending on whether a 2 or 3-digit MNC is used (see 3GPP TS 31.102 [27]) and separate them into MCC and MNC; if the MNC is 2-digit MNC then a zero shall be added at the beginning.
2. Use the MCC and MNC derived in step 1 to create the "mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org" domain name.
3. Add the label "prose-function." to the beginning of the domain.

An example of a Home PLMN ProSe Function address is:

IMSI in use: 234150999999999;

where:

- MCC = 234;
- MNC = 15; and
- MSIN = 0999999999,

which gives the following Home PLMN ProSe Function address:

"prose-function.mnc015.mcc234.pub.3gppnetwork.org".

24.6 ProSe Restricted Code

The ProSe Restricted Code as described in 3GPP TS 23.303 [103] is a single 64-bit identifier that corresponds to one or more Restricted ProSe Application User ID(s) (as defined in 3GPP TS 23.303 [103]). The exact content of the identifier is not specified in 3GPP.

24.7 ProSe Restricted Code Prefix

The ProSe Restricted Code Prefix as described in 3GPP TS 23.303 [103] is a ProSe Restricted Code which to be used with a ProSe Restricted Code Suffix. It shall have the same size and format as the ProSe Restricted Code.

24.8 ProSe Restricted Code Suffix

The ProSe Restricted Code Suffix as described in 3GPP TS 23.303 [103] is an identifier to be appended to a ProSe Restricted Code Prefix. Depending on the application configuration, the bit length of a ProSe Restricted Code Suffix varies from 8 to 120, incremented by multiples of 8.

24.9 ProSe Query Code

The ProSe Query Code as described in 3GPP TS 23.303 [103] is a ProSe Restricted Code allocated by the ProSe Function to the Discoverer UE for restricted ProSe direct discovery model B. The format of the ProSe Query Code is the same as that of the ProSe Restricted Code defined in clause 24.6.

24.10 ProSe Response Code

The ProSe Response Code as described in 3GPP TS 23.303 [103] is a ProSe Restricted Code allocated by the ProSe Function to the Discoveree UE for restricted ProSe direct discovery model B. The format of the ProSe Response Code is the same as that of the ProSe Restricted Code defined in clause 24.6.

24.11 ProSe Discovery UE ID

24.11.1 General

The ProSe Discovery UE ID as described in 3GPP TS 23.303 [103] identifies the UE participating in restricted ProSe direct discovery in the context of the ProSe Function.

It is composed of two parts as follows:

- The PLMN ID of the ProSe Function that assigned the ProSe Discovery UE ID, i.e. Mobile Country Code (MCC) and Mobile Network Code (MNC).
- A temporary identifier allocated by the ProSe Function. The content of the temporary identifier is not specified in 3GPP.

24.11.2 Format of ProSe Discovery UE ID

The ProSe Discovery UE ID is a bit string whose value is allocated by the ProSe Function. The length of the ProSe Discovery UE ID is equal to 64 bits and the format is described as shown in Figure 24.11.2-1.

Figure 24.11.2-1: Structure of ProSe Discovery UE ID

24.12 ProSe UE ID

The ProSe UE ID as described in 3GPP TS 23.303 [103] identifies the link layer address used for ProSe direct communication by a ProSe-enabled Public Safety UE.

The format of ProSe UE ID is a bit string whose length is equal to 24 bits.

24.13 ProSe Relay UE ID

The ProSe Relay UE ID as described in 3GPP TS 23.303 [103] identifies the link layer address used for ProSe direct communication by a ProSe UE-to-network relay UE.

The format of ProSe Relay UE ID is a bit string whose length is equal to 24 bits.

24.14 User Info ID

The User Info ID as described in 3GPP TS 23.303 [103] is used to identify the user information to be discovered for public safety use case. The value of User Info ID is allocated either by the operator or 3rd-party public safety provider application server.

The format of the User Info ID is a 48-bit bit-string.

24.15 Relay Service Code

The Relay Service Code as described in 3GPP TS 23.303 [103] identifies a connectivity service the ProSe UE-to-network relay provides.

The format of the Relay Service Code is a 24-bit bit-string.

24.16 Discovery Group ID

The Discovery Group ID as described in 3GPP TS 23.303 [103] identifies a group of Public Safety users that are affiliated for Group Member Discovery.

The format of the Discovery Group ID is a 24-bit bit-string.

24.17 Service ID

The Service ID is specified in 3GPP TS 23.303 [103], Annex C and specifies the 3GPP service category for ProSe. The Service ID shall be the string "3GPP ProSe Service Category".

25 Identification of Online Charging System

25.1 Introduction

This clause describes the format of the home network domain name of the Online Charging System (OCS), needed to access the Online Charging System. For further information on the use of this home network domain name, see 3GPP TS 29.212 [106]. For more information on the ".3gppnetwork.org" domain name and its applicability, see Annex D of the present document.

25.2 Home network domain name

The home network domain name of the OCS shall be in the form of an Internet domain name, e.g. operator.com, as specified in IETF RFC 1035 [19] and IETF RFC 1123 [20]. The home network domain of the OCS consists of one or more labels. Each label shall consist of the alphabetic characters (A-Z and a-z), digits (0-9) and the hyphen (-) in accordance with IETF RFC 1035 [19]. Each label shall begin and end with either an alphabetic character or a digit in accordance with IETF RFC 1123 [20]. The case of alphabetic characters is not significant.

If the home network domain of the OCS is not known (e.g. through an available static address or through its reception from another node), it shall be:

- in the form of "ocs.mnc<MNC>.mcc<MCC>.3gppnetwork.org", where "<MNC>" and "<MCC>" fields correspond to the MNC and MCC of the operator's PLMN to which the OCS belongs. Both the "<MNC>" and "<MCC>" fields are 3 digits long. If the MNC of the PLMN is 2 digits, then a zero shall be added at the beginning; and
- derived from the subscriber's IMSI, as described in the following steps:

  1. take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used (see 3GPP TS 31.102 [27]) and separate them into MCC and MNC; if the MNC is 2 digits then a zero shall be added at the beginning;
  2. use the MCC and MNC derived in step 1 to create the "mnc<MNC>.mcc<MCC>.3gppnetwork.org" domain name;
  3. add the label "ocs" to the beginning of the domain name.

An example of a home network domain name is:

IMSI in use: 234150999999999;

Where:

MCC = 234;

MNC = 15;

MSIN = 0999999999;

Which gives the home network domain name: ocs.mnc015.mcc234.3gppnetwork.org.

NOTE: It is implementation dependent to determine that the length of the MNC is 2 or 3 digits.

26 Numbering, addressing and identification for Mission Critical Services

26.1 Introduction

This clause describes the format of the parameters used for Mission Critical Services.

For further information on the use of the parameters see 3GPP TS 23.280 [114].

26.2 Domain name for MC services confidentiality protection of MC services identities

A Domain Name for MC Services confidentiality protection used in a host part of a SIP URI indicates that the user part of the SIP URI contains a confidentiality protected MC Services identity. This Domain Name shall be the string "mc1-encrypted.3gppnetwork.org".

Protected MCPTT identities are constructed according to 3GPP TS 24.379 [111].

Protected MCData identities are constructed according to 3GPP TS 24.282 [116].

Protected MCVideo identities are constructed according to 3GPP TS 24.281 [115].

27 Numbering, addressing and identification for V2X

27.1 Introduction

This clause describes the format of the parameters used for V2X. For further information on the use of the parameters see 3GPP TS 23.285 [117].

27.2 V2X Control Function FQDN

27.2.1 General

In order to retrieve V2X communication parameters, the UE needs to connect to the V2X Control Function. The address of the V2X control Function can be provisioned to the UE, or the UE can be pre-configured with the FQDN of the V2X Control Function. If the address of the V2X Control Function is not provisioned, and the UE is not pre-configured with the FQDN of the V2X Control Function FQDN, the UE self-constructs the V2X Control Function FQDN as per the format specified in clause 27.2.2.

27.2.2 Format of V2X Control Function FQDN

The V2X Control Function Fully Qualified Domain Name (V2X Control Function FQDN) contains an Operator Identifier that shall uniquely identify the PLMN where the V2X Control Function is located. The V2X Control Function FQDN is composed of six labels. The last two labels shall be "3gppnetwork.org". The third and fourth labels together shall uniquely identify the PLMN. The first two labels shall be "v2xcontrolfunction.epc". The result of the V2X Control Function FQDN will be:

"v2xcontrolfunction.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org"

In order to guarantee inter-PLMN DNS translation, the <MNC> and <MCC> coding used in the "v2xcontrolfunction.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org" format of the V2X Control Function FQDN shall be:

- <MNC> = 3 digits
- <MCC> = 3 digits

If there are only 2 significant digits in the MNC, one "0" digit shall be inserted at the left side to fill the 3 digits coding of MNC in the V2X Control Function FQDN.

As an example, the V2X Control Function FQDN for MCC 345 and MNC 12 is coded in the DNS as:

"v2xcontrolfunction.epc.mnc012.mcc345.3gppnetwork.org".

28 Numbering, addressing and identification for 5G System (5GS)

28.1 Introduction

Editor's note: This clause provides general description on numbering, addressing and identification for 5G core network.

This clause describes the format of the parameters, identifiers and information used for the 5G system. For further information on these, see 3GPP TS 23.501 [119], 3GPP TS 23.502 [120] and 3GPP TS 23.503 [121].

28.2 Home Network Domain

The Home Network Domain for 5GC shall be in the format specified in IETF RFC 1035 [19] and IETF RFC 1123 [20] and shall be structured as:

"5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org",

where "<MNC>" and "<MCC>" fields correspond to the MNC and MCC of the operator's PLMN. Both the "<MNC>" and "<MCC>" fields are 3 digits long. If there are only 2 significant digits in the MNC, one "0" digit shall be inserted at the left side to fill the 3 digits coding of MNC in the NF service endpoint format for inter PLMN routing.

As an example, the Home Network Domain for MCC 345 and MNC 12 is coded as:

"5gc.mnc012.mcc345.3gppnetwork.org".

28.3 Identifiers for Domain Name System procedures

28.3.1 Introduction

Editor's note: This clause will describe Domain Name System (DNS) related identifiers for 5GS used by the procedures specified in 3GPP TS 29.303.

28.3.2 Fully Qualified Domain Names (FQDNs)

28.3.2.1 General

Editor's note: This clause provides general information regarding DNS and FQDN.

28.3.2.2 N3IWF FQDN

28.3.2.2.1 General

The N3IWF Fully Qualified Domain Name (N3IWF FQDN) shall be constructed using one of the following formats, as specified in clause 6.3.6 of 3GPP TS 23.501 [119]:

- Operator Identifier based N3IWF FQDN;
- Tracking Area Identity based N3IWF FQDN;
- the N3IWF FQDN configured in the UE by the HPLMN.

NOTE: The N3IWF FQDN configured in the UE can have a different format than those specified in the following clauses.

The Visited Country FQDN for N3IWF is used by a roaming UE to determine whether the visited country mandates the selection of an N3IWF in this country. The Visited Country FQDN for N3IWF shall be constructed as specified in

clause 28.3.2.2.4. The Replacement field used in DNS-based Discovery of regulatory requirements shall be constructed as specified in clause 28.3.2.2.5.

Editor's note: It is FFS whether N3IWF FQDN for emergency service is supported.

28.3.2.2.2 Operator Identifier based N3IWF FQDN

The N3IWF Fully Qualified Domain Name (N3IWF FQDN) contains an Operator Identifier that shall uniquely identify the PLMN where the N3IWF is located. The N3IWF FQDN is composed of seven labels. The last three labels shall be "pub.3gppnetwork.org". The third and fourth labels together shall uniquely identify the PLMN. The first two labels shall be "n3iwf.5gc". The result of the N3IWF FQDN will be:

"n3iwf.5gc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org"

In the roaming case, the UE can utilise the services of the VPLMN or the HPLMN. In this case, the Operator Identifier based N3IWF FQDN shall be constructed as described above, but using the MNC and MCC of the VPLMN or the HPLMN.

In order to guarantee inter-PLMN DNS translation, the <MNC> and <MCC> coding used in the "n3iwf.5gc. mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org" format of the Operator Identifier based N3IWF FQDN shall be:

- <MNC> = 3 digits
- <MCC> = 3 digits

If there are only 2 significant digits in the MNC, one "0" digit shall be inserted at the left side to fill the 3 digits coding of MNC in the N3IWF FQDN.

As an example, the Operator Identifier based N3IWF FQDN for MCC 345 and MNC 12 is coded in the DNS as:

"n3iwf.5gc.mnc012.mcc345.pub.3gppnetwork.org".

28.3.2.2.3 Tracking Area Identity based N3IWF FQDN

The Tracking Area Identity based N3IWF FQDN is used to support location based N3IWF selection within a PLMN.

There are two N3IWF FQDNs defined one based on a TAI with a 2 octet TAC and a 5GS one based on a 3 octet TAC.

1) The Tracking Area Identity based N3IWF FQDN using a 2 octet TAC shall be constructed respectively as:

"tac-lb<TAC-low-byte>.tac-hb<TAC-high-byte>.tac.n3iwf.5gc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org"

where

- the <MNC> and <MCC> shall identify the PLMN where the N3IWF is located and shall be encoded as
  - <MNC> = 3 digits
  - <MCC> = 3 digits

  If there are only 2 significant digits in the MNC, one "0" digit shall be inserted at the left side to fill the 3 digits coding of MNC in the N3IWF FQDN.
- the <TAC>, together with the <MCC> and <MNC> shall identify the Tracking Area Identity the UE is located in.

  The TAC is a 16-bit integer. The <TAC-high-byte> is the hexadecimal string of the most significant byte in the TAC and the <TAC-low-byte > is the hexadecimal string of the least significant byte. If there are less than 2 significant digits in <TAC-high-byte> or <TAC-low-byte >, "0" digit(s) shall be inserted at the left side to fill the 2 digit coding;

As examples,

- the Tracking Area Identity based N3IWF FQDN for the TAC H'0B21, MCC 345 and MNC 12 is coded in the DNS as:

"tac-lb21.tac-hb0b.tac.n3iwf.5gc.mnc012.mcc345.pub.3gppnetwork.org"

2) The 5GS Tracking Area Identity based N3IWF FQDN using a 3 octet TAC shall be constructed respectively as:

"tac-lb<TAC-low-byte>.tac-mb<TAC-middle-byte>.tac-hb<TAC-high-byte>.5gstac.n3iwf.5gc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org"

where

- the <MNC> and <MCC> shall identify the PLMN where the N3IWF is located and shall be encoded as
  - <MNC> = 3 digits
  - <MCC> = 3 digits

  If there are only 2 significant digits in the MNC, one "0" digit shall be inserted at the left side to fill the 3 digits coding of MNC in the N3IWF FQDN.

- the <TAC>, together with the <MCC> and <MNC> shall identify the 5GSTracking Area Identity the UE is located in.

  The 5GS TAC is a 24-bit integer. The <TAC-high-byte> is the hexadecimal string of the most significant byte in the TAC and the <TAC-low-byte > is the hexadecimal string of the least significant byte. If there are less than 2 significant digits in <TAC-low-byte>, <TAC-middle-byte> or <TAC-high-byte >, "0" digit(s) shall be inserted at the left side to fill the 2 digit coding;

As examples,

- the 5GS Tracking Area Identity based N3IWF FQDN for the 5GS TAC H'0B1A21, MCC 345 and MNC 12 is coded in the DNS as:

  "tac-lb21.tac-mb1a.tac-hb0b.5gstac.n3iwf.5gc.mnc012.mcc345.pub.3gppnetwork.org"

28.3.2.2.4 Visited Country FQDN for N3IWF

The Visited Country FQDN for N3IWF, used by a roaming UE to determine whether the visited country mandates the selection of an N3IWF in this country, shall be constructed as described below.

The Visited Country FQDN shall contain a MCC that uniquely identifies the country in which the UE is located.

The Visited Country FQDN is composed of seven labels. The last three labels shall be "pub.3gppnetwork.org". The fourth label shall be "visited-country". The third label shall uniquely identify the MCC of the visited country. The first and second labels shall be "n3iwf.5gc". The resulting Visited Country FQDN of N3IWF will be:

"n3iwf.5gc.mcc<MCC>.visited-country.pub.3gppnetwork.org"

The <MCC> coding used in this FQDN shall be:

- <MCC> = 3 digits

As an example, the Visited Country FQDN for MCC 345 is coded in the DNS as:

"n3iwf.5gc.mcc345.visited-country.pub.3gppnetwork.org".

28.3.2.2.5 Replacement field used in DNS-based Discovery of regulatory requirements

If the visited country mandates the selection of an N3IWF in this country, the NAPTR record(s) associated to the Visited Country FQDN shall be provisioned with the replacement field containing the identity of the PLMN(s) in the visited country which may be used for N3IWF selection.

The replacement field shall take the form of an Operator Identifier based N3IWF FQDN as specified in clause 28.3.2.2.2.

For countries with multiple MCC, the NAPTR records returned by the DNS may contain a different MCC than the MCC indicated in the Visited Country FQDN.

As an example, the NAPTR records associated to the Visited Country FQDN for MCC 345, and for MNC 012, 013 and 014, are provisioned in the DNS as:

```
n3iwf.5gc.mcc345.visited-country.pub.3gppnetwork.org
;     IN NAPTR    order     pref.flag service    regexp    replacement
      IN NAPTR    100  999  ""         ""    n3iwf.5gc.mnc012.mcc345.pub.3gppnetwork.org
      IN NAPTR    100  999  ""         ""    n3iwf.5gc.mnc013.mcc345.pub.3gppnetwork.org
      IN NAPTR    100  999  ""         ""    n3iwf.5gc.mnc014.mcc345.pub.3gppnetwork.org
```

28.3.2.3 PLMN level and Home NF Repository Function (NRF) FQDN

28.3.2.3.1 General

When an NF is instantiated, it may register with a PLMN level NF Repository Function (NRF). It may then discover other NF instance(s) in the 5GC by querying the PLMN level NRF. The IP address of the PLMN level NRF can be provisioned into the NF, or the NF can be pre-configured with the FQDN of the PLMN level NRF. If the PLMN level NRF addresses and FDQN are not provisioned into the NF, the NF self-constructs the PLMN level NRF FQDN as per the format specified in clause 28.3.2.3.2.

For NF discovery across PLMNs, the NRF (e.g vNRF) shall self-construct the PLMN level NRF FQDN of the target PLMN (e.g hNRF) as per the format specified in clause 28.3.2.3.2, and the hNRF URI as per the format specified in subsclause 28.3.2.3.3, if the NRF has not obtained the NRF FQDN of the target PLMN.

28.3.2.3.2 Format of NRF FQDN

The NRF FQDN shall be constructed by prefixing the Home Network Domain Name (see clause 28.2) of the PLMN in which the NRF is located with the label "nrf." as described below:

- nrf.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

28.3.2.3.3 NRF URI

In absence of any other local configuration available in the vNRF, the API URIs of the hNRF shall be constructed by deriving the API root (see 3GPP TS 29.501 [128]) as follows:

- the authority part shall be set to the NRF FQDN as specified in 28.3.2.3.2
- the scheme shall be "https"
- the port shall be the default port for the "https" scheme, i.e. 443.
- the API prefix optional component shall not be used

EXAMPLE: For an MCC = 012 and MNC = 345, the API root of the NRF services shall be:

"https://nrf.5gc.mnc345.mcc012.3gppnetwork.org/"

28.3.2.4 Network Slice Selection Function (NSSF) FQDN

28.3.2.4.1 General

For roaming service, the vNSSF may invoke the Nnssf_NSSelection_Get service operation from the hNSSF. For routing of the HTTP/2 messages across the PLMN, the vNSSF self-constructs the FQDN of the hNSSF as per the format specified in clause 28.3.2.4.2 and the URI of the hNSSF as per the format specified in clause 28.3.2.4.3. The Home Network is identified by the PLMN ID of the SUPI provided to the vNSSF by the NF Service Consumer (e.g. the AMF).

28.3.2.4.2 Format of NSSF FQDN

The NSSF FQDN shall be constructed by prefixing its Home Network Domain Name (see clause 28.2) with the label "nssf." as described below:

- nssf.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

28.3.2.4.3 NSSF URI

In absence of any other local configuration available in the vNSSF, the API URIs of the hNSSF shall be constructed by deriving the API root (see 3GPP TS 29.501 [128]) as follows:

- the authority part shall be set to the NSSF FQDN as specified in 28.3.2.4.2
- the scheme shall be "https"
- the port shall be the default port for the "https" scheme, i.e. 443.
- the API prefix optional component shall not be used

EXAMPLE: For an MCC = 012 and MNC = 345, the API root of the NSSF services shall be:

"https://nssf.5gc.mnc345.mcc012.3gppnetwork.org/"

28.3.2.5 AMF Name

The AMF Name FQDN shall uniquely identify an AMF.

The AMF Name FQDN shall be constructed as:

"<AMF-id>.amf.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org"

where

- the <MNC> and <MCC> shall identify the PLMN where the AMF is located and shall be encoded as
  - <MNC> = 3 digits
  - <MCC> = 3 digits

  If there are only 2 significant digits in the MNC, one "0" digit shall be inserted at the left side to fill the 3 digits coding of MNC in the AMF Name FQDN.
- the <AMF-id> shall contain at least one label.

As example,

- If <AMF-id> is amf1.cluster1.net2, the AMF Name FQDN for MCC 345 and MNC 12 as:

  "amf1.cluster1.net2.amf.5gc.mnc012.mcc345.3gppnetwork.org"

28.3.2.6 5GS Tracking Area Identity (TAI) FQDN

The 5GS Tracking Area Identity (TAI) FQDN shall be constructed as follows:

"tac-lb<TAC-low-byte>.tac-mb<TAC-middle-byte>.tac-hb<TAC-high-byte>.5gstac.
5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org"

where the <TAC>, together with the <MCC> and <MNC> shall identify the 5GS Tracking Area Identity, and shall be encoded as follows:

- <MNC> = 3 digits
- <MCC> = 3 digits

  If there are only 2 significant digits in the MNC, one "0" digit shall be inserted at the left side to fill the 3 digits coding of MNC in the 5GS TAI FQDN.
- The 5GS TAC is a 24-bit integer. The <TAC-high-byte> is the hexadecimal string of the most significant byte in the TAC and the <TAC-low-byte > is the hexadecimal string of the least significant byte. If there are less than 2 significant digits in <TAC-low-byte>, <TAC-middle-byte> or <TAC-high-byte >, "0" digit(s) shall be inserted at the left side to fill the 2 digits coding;

As an example, the 5GS Tracking Area Identity for the 5GS TAC H'0B1A21, MCC 345 and MNC 12 is coded in the DNS as:

"tac-lb21.tac-mb1a.tac-hb0b.5gstac.5gc.mnc012.mcc345.3gppnetwork.org"

28.3.2.7 AMF Set FQDN

An AMF Set within an operator's network is identified by its AMF Set ID, AMF Region ID, MNC and MCC.

A subdomain name shall be derived from the MNC and MCC by adding the label "amfset" to the beginning of the Home Network Realm/Domain (see clause 28.2).

The AMF Set FQDN shall be constructed as follows:

set<AMF Set Id>.region<AMF Region Id>.amfset.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

where

- <MNC> = 3 digits
- <MCC> = 3 digits

  If there are only 2 significant digits in the MNC, one "0" digit shall be inserted at the left side to fill the 3 digits coding of MNC in the AMF Set FQDN.

- <AMF Set Id> and <AMF Region Id> are the hexadecimal strings of the AMF Set ID and AMF Region ID. If there are less than 2 significant digits in <AMF Region Id>, "0" digit(s) shall be inserted at the left side to fill the 2 digits coding. If there are less than 3 significant digits in <AMF Set Id>, "0" digit(s) shall be inserted at the left side to fill the 3 digits coding.

As an example, the AMF Set FQDN for the AMF Set 1, AMF Region 48 (hexadecimal), MCC 345 and MNC 12 is coded as:

"set001.region48.amfset.5gc.mnc012.mcc345.3gppnetwork.org"

28.3.2.8 AMF Instance FQDN

The AMF Instance FQDN shall uniquely identify an AMF instance.

The AMF Instance FQDN shall be constructed as:

pt<AMF Pointer>.set<AMF Set Id>.region<AMF Region Id>.amfi.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

where

- <MNC> = 3 digits
- <MCC> = 3 digits

  If there are only 2 significant digits in the MNC, one "0" digit shall be inserted at the left side to fill the 3 digits coding of MNC in the AMF Instance FQDN.

- <AMF Pointer>, <AMF Set Id> and <AMF Region Id> are the hexadecimal strings of the AMF Pointer, AMF Set ID and AMF Region ID. If there are less than 2 significant digits in <AMF Pointer> or <AMF Region Id>, "0" digit(s) shall be inserted at the left side to fill the 2 digits coding of the AMF Pointer or AMF Region Id respectively. If there are less than 3 significant digits in <AMF Set Id>, "0" digit(s) shall be inserted at the left side to fill the 3 digits coding.

As an example, the AMF Instance FQDN for the AMF Pointer 12 (hexadecimal), AMF Set 1, AMF Region 48 (hexadecimal), MCC 345 and MNC 12 is coded as:

"pt12.set001.region48.amfi.5gc.mnc012.mcc345.3gppnetwork.org"

28.3.2.9 SMF Set FQDN

An SMF Set within an operator's network is identified by its NF Set ID as defined in clause 28.12, with NFType set to "SMF".

A subdomain name shall be derived from the MNC and MCC by adding the label "smfset" to the beginning of the Home Network Realm/Domain (see clause 28.2).

The SMF Set FQDN shall be constructed as follows:

set<Set Id>.smfset.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

where

- <MNC> = 3 digits
- <MCC> = 3 digits

  If there are only 2 significant digits in the MNC, one "0" digit shall be inserted at the left side to fill the 3 digits coding of MNC in the AMF Set FQDN.

- <Set Id> is the string representing the Set ID part within the NF Set ID defined in clause 28.12.

EXAMPLE: "set12. smfset.5gc.mnc012.mcc345.3gppnetwork.org" (for an SMF set from MCC 345, MNC 12 and SetID "12")

28.4 Information for Network Slicing

28.4.1 General

In order to identify a Network Slice end to end, the 5GS uses information called S-NSSAI (Single Network Slice Selection Assistance Information). See clause 5.15.2 of 3GPP TS 23.501 [119].

An S-NSSAI is comprised of:

- A Slice/Service type (SST),
- A Slice Differentiator (SD), which is optional information that complements the Slice/Service type(s) to differentiate amongst multiple Network Slices.

28.4.2 Format of the S-NSSAI

The structure of the S-NSSAI is depicted in Figure 28.4.2-1

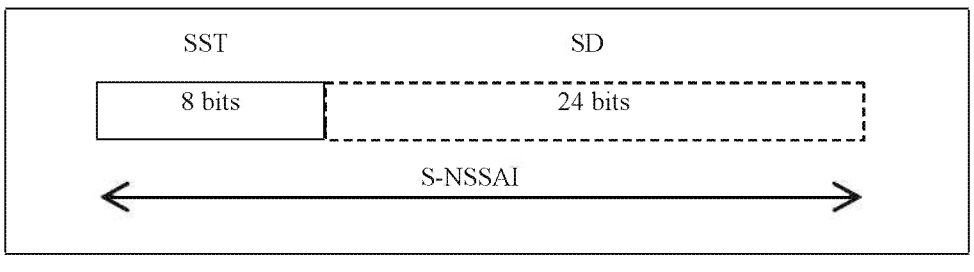

Figure 28.4.2-1: Structure of S-NSSAI

The S-NSSAI may include both the SST and SD fields (in which case the S-NSSAI length is 32 bits in total), or the S-NSSAI may just include the SST field (in which case the S-NSSAI length is 8 bits only).

The SST field may have standardized and non-standardized values. Values 0 to 127 belong to the standardized SST range and they are defined in 3GPP TS 23.501 [119]. Values 128 to 255 belong to the Operator-specific range.

The SD field has a reserved value "no SD value associated with the SST" defined as hexadecimal FFFFFF.

The SD field has a reserved value "no SD value associated with the SST" defined as hexadecimal FFFFFF.

28.5 NF FQDN Format for Inter PLMN Routing

28.5.1 General

For routing HTTP/2 request messages to NF in a different PLMN, the FQDN of the target NF shall have the Home Network Domain (see clause 28.2) as the trailing part.

28.5.2 Telescopic FQDN

The FQDN of the NF services or the authority part of URIs in another PLMN, may be appended with the PLMN Network Domain of the request initiating PLMN, as the trailing part to form a Telescopic FQDN as specified in 3GPP TS 33.501 [124]. The structure of the Telescopic FQDN is as specified below:

<Label representing FQDN from other PLMN>.<FQDN of the SEPP in the request initiating PLMN>,

where:

- FQDN from other PLMN is the FQDN of the other PLMN NF (for e.g. returned in the NF Discovery Response) or the authority part of URIs from other PLMN, which may be rewritten by the other PLMN SEPP for topology hiding. The request initiating PLMN SEPP shall replace the other PLMN FQDN with a label;

NOTE 1: How a SEPP constructs the label to replace the other PLMN FQDN is implementation specific. The label replacement is required in order to avoid multiple subdomains in the FQDN since the SEPP presents wildcard certificates on behalf of the other PLMN and only single level subdomain is allowed in a wildcard certificate as per IETF RFC 2818 [127].

NOTE 2: FQDN from other PLMN includes the network domain of the other PLMN.

- FQDN of the SEPP in the request initiating PLMN is the identifier of the SEPP in the request initaiting PLMN (e.g. VPLMN).

28.6 5GS Tracking Area Identity (TAI)

The 5GS Tracking Area Identity (TAI) consists of a Mobile Country Code (MCC), Mobile Network Code (MNC), and Tracking Area Code (TAC). It is composed as shown in figure 28.6.1.

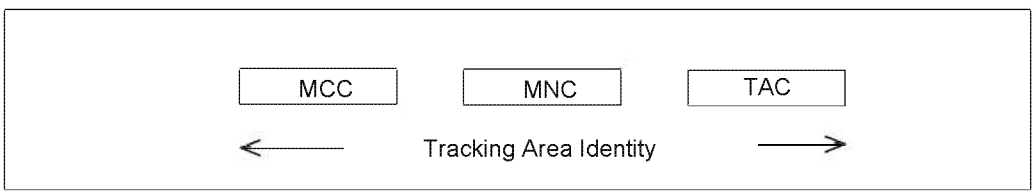

Figure 28.6.1: Structure of the 5GS Tracking Area Identity (TAI)

The TAI is composed of the following elements:

- Mobile Country Code (MCC) identifies the country in which the PLMN is located. The value of the MCC is the same as the 3-digit MCC contained in the IMSI;

- Mobile Network Code (MNC) is a code identifying the PLMN in that country. The value of the MNC is the same as the 2-digit or 3-digit MNC contained in the IMSI;

- 5GS Tracking Area Code (TAC) is a fixed length code (of 3 octets) identifying a Tracking Area within a PLMN. This part of the tracking area identification shall be coded using a full hexadecimal representation. The following are reserved hexadecimal values of the TAC:
  - 000000, and
  - FFFFFE.

NOTE: The above reserved values are used in some special cases when no valid TAI exists in the UE (see 3GPP TS 24.501 [125] for more information).

28.7 Network Access Identifier (NAI)

28.7.1 Introduction

This clause describes the NAI formats used in the 5G System.

28.7.2 NAI format for SUPI

A SUPI containing a network specific identifier shall take the form of a Network Access Identifier (NAI).

The NAI for SUPI shall have the form username@realm as specified in clause 2.2 of IETF RFC 7542 [126].See clause 5.9.2 of 3GPP TS 23.501 [119] for the definition and use of the network specific identifier.

28.7.3 NAI format for SUCI

When the SUPI is defined as a Network Specific Identifier, the SUCI shall take the form of a Network Access Identifier (NAI). In this case, the NAI format of the SUCI shall have the form username@realm as specified in clause 2.2 of IETF RFC 7542 [126], where the realm part shall be identical to the realm part of the Network Specific Identifier.

When the SUPI is defined as an IMSI, the SUCI in NAI format shall have the form username without a realm part as specified in clause 2.2 of IETF RFC 7542 [126].

The username part of the NAI shall take one of the following forms:

a) for the null-scheme:

   type<supi type>.rid<routing indicator>.schid<protection scheme id>.userid<MSIN or Network Specific Identifier SUPI username>

b) for the Scheme Output for Elliptic Curve Integrated Encryption Scheme Profile A and Profile B:

   type<supi type>.rid<routing indicator>.schid<protection scheme id>.hnkey<home network public key id>.ecckey<ECC ephemeral public key value>.cip<ciphertext value>.mac<MAC tag value>

c) for HPLMN proprietary protection schemes:

   type<supi type>.rid<routing indicator>.schid<protection scheme id>.hnkey<home network public key id>.out<HPLMN defined scheme output>

See clause 2.2B for the definition and format of the different fields of the SUCI.

Examples:

Assuming the IMSI 234150999999999, where MCC=234, MNC=15 and MSISN=0999999999, the Routing Indicator 678, and a Home Network Public Key Identifier of 27, the NAI format for the SUCI takes the form:

- for the null-scheme:

  type0.rid678.schid0.userid0999999999

- for the Profile <A> protection scheme:

type0.rid678.schid1.hnkey27.ecckey<ECC ephemeral public key>.cip< encryption of 0999999999>.mac<MAC tag value>

Assuming the Network Specific Identifier user17@example.com, the Routing Indicator 678, and a Home Network Public Key Identifier of 27, the NAI format for the SUCI takes the form:

- for the null-scheme:

  type1.rid678.schid0.useriduser17@example.com

- for the Profile <A> protection scheme:

  type1.rid678.schid1.hnkey27.ecckey<ECC ephemeral public key>.cip< encryption of user17>.mac<MAC tag value>@example.com

28.7.4 Emergency NAI for Limited Service State

This clause describes the format of the UE identification when UE is performing an emergency registration and IMSI is not available or not authenticated.

The Emergency NAI for Limited Service State shall take the form of an NAI, and shall have the form username@realm as specified in clause 2.2 of IETF RFC 7542 [126]. The exact format shall be:

imei<IMEI>@sos.invalid

NOTE: The top level domain ".invalid" is a reserved top level domain, as specified in IETF RFC 2606 [64], and is used here due to the fact that this NAI never needs to be resolved for routing.

or if IMEI is not available,

mac<MAC>@sos.invalid

For example, if the IMEI is 219551288888888, the Emergency NAI for Limited Service State then takes the form of imei219551288888888@sos.invalid.

For example, if the MAC address is 44-45-53-54-00-AB, the Emergency NAI for Limited Service State then takes the form of mac4445535400AB@sos.invalid, where the MAC address is represented in hexadecimal format without separators.

28.7.5 Alternative NAI

The Alternative NAI shall take the form of a NAI, i.e. 'any_username@realm' as specified of IETF RFC 7542 [126]. The Alternative NAI shall not be routable from any AAA server.

The Alternative NAI shall contain a username part that is not a null string.

The realm part of the NAI shall be "unreachable.3gppnetwork.org".

The result shall be an NAI in the form of:

"<any_non_null_string>@unreachable.3gppnetwork.org".

28.8 Generic Public Subscription Identifier (GPSI)

The Generic Public Subscription Identifier (GPSI) is defined in clause 5.9.8 of 3GPP TS 23.501 [119].

The GPSI is defined as:

- a GPSI type: in this release of the specification, it may indicate an MSISDN or an External Identifier; and
- dependent on the value of the GPSI type:
  - an MSISDN as defined in clause 3.3; or

- an External Identifier as defined in clause 19.7.2.

NOTE: Depending on the protocol used to convey the GPSI, the GPSI type can take different formats.

28.9 Internal-Group Identifier

Internal-Group Identifier is a network internal globally unique ID which identifies a set of SUPIs (e.g. MTC devices) from a given network that are grouped together for one specific group related service (see 3GPP TS 23.501 [119] clause 5.9.7).

An Internal-Group Identifier shall be composed in the same way as IMSI-Group Identifier (see clause 19.9).

If a 5G subscriber's IMSI belongs to an IMSI-Group identified by a given IMSI-Group Identifier X, the IMSI shall also belong to the Internal-Group identified by the Internal-Group Identifier X.

28.10 Presence Reporting Area Identifier (PRA ID)

The Presence Reporting Area Identifier (PRA ID) is used to identify a Presence Reporting Area (PRA).

PRAs can be used for reporting changes of UE presence in a PRA, e.g. for policy control or charging decisions. See 3GPP TS 23.501 [119] and 3GPP TS 23.503 [121].

A PRA is composed of a short list of TAs and/or NG-RAN nodes and/or cells identifiers in a PLMN.A PRA can be:

- either a "UE-dedicated PRA", defined in the subscriber profile;
- or a "Core Network predefined PRA", pre-configured in AMF.

PRA IDs used to identify "Core Network predefined PRAs" shall not be used for identifying "UE-dedicated PRAs".

The same PRA ID may be used for different UEs to identify different "UE-dedicated PRAs", i.e. PRA IDs may overlap between different UEs, while identifying different "UE-dedicated PRAs".

The PRA ID shall be formatted as an integer within the following ranges:

0 .. 8 388 607 for UE-dedicated PRA

8 388 608 to 16 777 215 for Core Network predefined PRA.

NOTE: The PRA ID is encoded over the Service Based Interfaces as a string of digits representing an integer. See 3GPP TS 29.571 [129].

28.11 CAG-Identifier

A Closed Access Group (CAG) within a PLMN is uniquely identified by a CAG-Identifier (see 3GPP TS 23.501 [119]).

The CAG-Identifier shall be a fixed length 32 bit value.

Editor's Note: The length is to be confirmed by RAN2

28.12 NF Set Identifier (NF Set ID)

A NF Set Identifier is a globally unique identifier of a set of equivalent and interchangeable CP NFs from a given network to provide distribution, redundancy and scalability (see clause 5.21.3 of 3GPP TS 23.501 [119]).

An NF Set Identifier shall be constructed from the MCC, MNC, NF type and a Set ID.

A NF Set Identifier is formatted as the following string

<NF Set ID> = <MCC>_<MNC>_<NFType>_<Set ID>

where:

- the MCC and MNC identify the PLMN of the NF Set;
- the NFType identifies the NF type of the NFs within the NF set, as defined by 3GPP TS 29.510 [x];
- the Set ID is a NF type specific Set ID within the PLMN, chosen by the operator and defined as a string of characters other than the delimiter "_".

  For an AMF set, the Set ID shall be set to "region<AMF Region ID>-set<AMF Set ID>", with the AMF Region ID and AMF Set ID encoded as defined in 3GPP TS 29.571 [129].

EXAMPLE 1: 345_12_SMF_set1

EXAMPLE 2: 345_12_PCF_12

EXAMPLE 3: 345_12_AMF_region48-set001 (for AMF Region 48 (hexadecimal) and AMF Set 1)

Editor's Note: the exact format of the NF Set ID, e.g. as specified above or as an FQDN, is FFS.

Editor's Note: other characters, e.g. white space, may also need to be restricted from the Set ID.

28.13 NF Service Set Identifier (NF Service Set ID)

A NF Service Set Identifier is a globally unique identifier of a set of equivalent and interchangeable CP NF service instances within a NF instance from a given network to provide distribution, redundancy and scalability (see clause 5.21.3 of 3GPP TS 23.501 [119]).

An NF Service Set Identifier shall be constructed from the MCC, MNC, NF instance Identifier, service name and a Set ID.

A NF Service Set Identifier is formatted as the following string

<NF Service Set ID> = <MCC>_<MNC>_<NFInstanceID>_<ServiceName>_<Set ID>

where:

- the MCC and MNC identify the PLMN of the NF Service Set;
- the NFInstanceID identifies the NF instance of the NF Service set, as defined by 3GPP TS 23.501 [119] and 3GPP TS 29.510 [130];
- the ServiceName identifies the NF service of the NF Service set, as defined by 3GPP TS 29.510 [130];
- the Set ID is a service specific Set ID within the NF instance, chosen by the operator and defined as a string of characters other than the delimiter "_".

EXAMPLE 1: 345_12_ 54804518-4191-46b3-955c-ac631f953ed8_nsmf-pdusession_set-3

EXAMPLE 2: 345_12_ 54804518-4191-46b3-955c-ac631f953ed8_npcf-smpolicycontrol_2

NF service instances from different NF instances are equivalent NF service instances if they share the same MCC, MNC, ServiceName and Set ID.

Editor's Note: the exact format of the NF Service Set ID, e.g. as specified above or as an FQDN, is FFS.

Editor's Note: other characters, e.g. white space, may also need to be restricted from the Set ID.

29 Numbering, addressing and identification for RACS

29.1 Introduction

This clause describes the format of the parameters used for Radio Capability Signalling Optimisation (RACS). For further information on the use of the parameters see 3GPP TS 23.401 [72] and 3GPP TS 23.501 [119].

29.2 UE radio capability ID

The UE radio capability ID is composed as shown in figure 29.2-1.

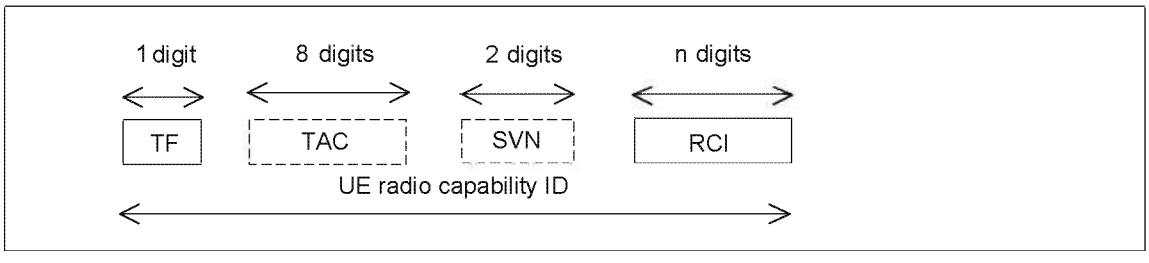

Figure 29.2-1: Structure of UE radio capability ID

The UE radio capability ID is composed of the following elements (each element shall consist of decimal digits only):

1) Type Field (TF): identifies the type of UE radio capability ID. The following values are defined:
   - 0: manufacturer-assigned UE radio capability ID;
   - 1: network-assigned UE radio capability ID with TAC and SVN fields;
   - 2: network-assigned UE radio capability ID without TAC and SVN fields; and
   - 3 to 9: spare values for future use.
2) Type Allocation Code (TAC). Its length is 8 digits. This field is present only if the Type Field is set to 0 or 1;
3) Software Version Number (SVN): identifies the software version number of the mobile equipment. Its length is 2 digits. This field is present only if the Type Field is set to 0 or 1;
4) Radio Configuration Identifier (RCI): identifies the UE radio configuration. Its length is n digits.

Editor's note [WI: RACS, CR#0543]: The value of n is FFS.

Editor's note [WI: RACS, CR#0543]: Whether a restart counter needs to be included in the UE radio capability ID is FFS.

Annex A (informative): Colour Codes

A.1 Utilization of the BSIC

A BSIC is allocated to each cell. A BSIC can take one of 64 values. In each cell the BSIC is broadcast in each burst sent on the SCH, and is then known by all MSs which synchronise with this cell. The BSIC is used by the MS for several purposes, all aiming at avoiding ambiguity or interference which can arise when an MS in a given position can receive signals from two cells *using the same BCCH frequency*.

Some of the uses of the BSIC relate to cases where the MS is attached to one of the cells. Other uses relate to cases where the MS is attached to a third cell, usually somewhere between the two cells in question.

The first category of uses includes:

- The three least significant bits of the BSIC indicate which of the 8 training sequences is used in the bursts sent on the downlink common channels of the cell. Different training sequences allow for a better transmission if

there is interference. The group of the three least significant bits of the BSIC is called the BCC (Base station Colour Code).

- The BSIC is used to modify the bursts sent by the MSs on the access bursts. This aims to avoid one cell correctly decoding access bursts sent to another cell.

The second category of uses includes:

- When in connected mode, the MSs measure and report the level they receive on a number of frequencies, corresponding to the BCCH frequencies of neighbouring cells in the same network as the used cell. Along with the measurement result, the MS sends to the network the BSIC which it has received on that frequency. This enables the network to discriminate between several cells which happen to use the same BCCH frequency. Poor discrimination might result in faulty handovers.

- The content of the measurement report messages is limited to information for 6 neighbour cells. It is therefore useful to limit the reported cells to those to which handovers are accepted. For this purpose, each cell provides a list of the values of the three most significant bits of the BSICs which are allocated to the cells which are useful to consider for handovers (usually excluding cells in other PLMNs). This information enables the MS to discard information for cells with non-conformant BSICs and not to report them. The group of the three most significant bits of the BSIC is called the NCC (Network Colour Code).

It should be noted that when in idle mode, the MS identifies a cell (for cell selection purposes) according to the cell identity broadcast on the BCCH and *not* by the BSIC.

A.2 Guidance for planning

From these uses, the following planning rule can be derived:

If there exist places where MSs can receive signals from two cells, whether in the same PLMN or in different PLMNs, which use the same BCCH frequency, it is highly preferable that these two cells have different BSICs.

Where the coverage areas of two PLMNs overlap, the rule above is respected if:

1) The PLMNs use different sets of BCCH frequencies (In particular, this is the case if no frequency is common to the two PLMNs. This usually holds for PLMNs in the same country), or

2) The PLMNS use different sets of NCCs, or

3) BSIC and BCCH frequency planning is co-ordinated.

Recognizing that method 3) is more cumbersome than method 2), and that method 1) is too constraining, it is suggested that overlapping PLMNs which use a common part of the spectrum agree on different NCCs to be used in any overlapping areas. As an example, a preliminary NCC allocation for countries in the European region can be found in clause A.3 of this annex.

This example can be used as a basis for bilateral agreements. However, the use of the NCCs allocated in clause A.3 is not compulsory. PLMN operators can agree on different BSIC allocation rules in border areas. The use of BSICs is not constrained in non-overlapping areas, or if ambiguities are resolved by using different sets of BCCH frequencies.

If the PLMNs share one or more cells with other PLMNs, the planning rule above should be applied also when the BCCH frequency is different. The rule should be respected by using different sets of NCCs. In addition to that, the PLMN sharing one or more cells with other PLMNs should use different NCCs for shared and non-shared neighbouring cells.

A.3 Example of PLMN Colour Codes (NCCs) for the European region

Austria	:	0
Belgium	:	1
Cyprus	:	3

Denmark	:	1
Finland	:	0
France	:	0
Germany	:	3
Greece	:	0
Iceland	:	0
Ireland	:	3
Italy	:	2
Liechtenstein	:	2
Luxembourg	:	2
Malta	:	1
Monaco	:	3 (possibly 0(=France))
Netherlands	:	0
Norway	:	3
Portugal	:	3
San Marino	:	0 (possibly 2(= Italy))
Spain	:	1
Sweden	:	2
Switzerland	:	1
Turkey	:	2
UK	:	2
Vatican	:	1 (possibly 2(=Italy)
Yugoslavia	:	3

This allows a second operator for each country by allocating the colour codes n (in the table) and n + 4. More than 2 colour codes per country may be used provided that in border areas only the values n and/or n+4 are used.

Annex B (normative): IMEI Check Digit computation

B.1 Representation of IMEI

The International Mobile station Equipment Identity and Software Version number (IMEISV), as defined in clause 6, is a 16 digit decimal number composed of three distinct elements:

- an 8 digit Type Allocation Code (TAC);
- a 6 digit Serial Number (SNR); and
- a 2 digit Software Version Number (SVN).

The IMEISV is formed by concatenating these three elements as illustrated below:

Figure A.1: Composition of the IMEISV

The IMEI is complemented by a check digit as defined in clause 3. The Luhn Check Digit (CD) is computed on the 14 most significant digits of the IMEISV, that is on the value obtained by ignoring the SVN digits.

The method for computing the Luhn check is defined in Annex B of the International Standard "Identification cards - Numbering system and registration procedure for issuer identifiers" (ISO/IEC 7812 [3]).

In order to specify precisely how the CD is computed for the IMEI, it is necessary to label the individual digits of the IMEISV, excluding the SVN. This is done as follows:

The (14 most significant) digits of the IMEISV are labelled D14, D13 ... D1, where:

- TAC = D14, D13 ... D7 (with D7 the least significant digit of TAC);
- SNR = D6, D5 ... D1 (with D1 the least significant digit of SNR).

B.2 Computation of CD for an IMEI

Computation of CD from the IMEI proceeds as follows:

Step 1: Double the values of the odd labelled digits D1, D3, D5 ... D13 of the IMEI.

Step 2: Add together the individual digits of all the seven numbers obtained in Step 1, and then add this sum to the sum of all the even labelled digits D2, D4, D6 ... D14 of the IMEI.

Step 3: If the number obtained in Step 2 ends in 0, then set CD to be 0. If the number obtained in Step 2 does not end in 0, then set CD to be that number subtracted from the next higher number which does end in 0.

B.3 Example of computation

IMEI (14 most significant digits):

TAC								SNR					
D14	D13	D12	D11	D10	D9	D8	D7	D6	D5	D4	D3	D2	D1
2	6	0	5	3	1	7	9	3	1	1	3	8	3

Step 1:

2	6	0	5	3	1	7	9	3	1	1	3	8	3
x2	x2	x2	x2					x2	x2	x2			
12	10	2	18					2	6	6			

Step 2:

2 + 1 + 2 + 0 + 1 + 0 + 3 + 2 + 7 + 1 + 8 + 3 + 2 + 1 + 6 + 8 + 6 = 53

Step 3:

CD = 60 - 53 = 7

Annex C (normative): Naming convention

This normative annex defines a naming convention which will make it possible for DNS servers to translate logical names for GSNs and RAs to physical IP addresses. The use of logical names is optional, but if the option is used, it shall comply with the naming convention described in this annex. The fully qualified domain names used throughout this annex shall follow the general encoding rules specified in clause 19.4.2.1.

C.1 Routing Area Identities

This clause describes a possible way to support inter-PLMN roaming.

When an MS roams between two SGSNs within the same PLMN, the new SGSN finds the address of the old SGSN from the identity of the old RA. Thus, each SGSN can determine the address of every other SGSN in the PLMN.

When an MS roams from an SGSN in one PLMN to an SGSN in another PLMN, the new SGSN may be unable to determine the address of the old SGSN. Instead, the SGSN transforms the old RA information to a logical name of the form:

racAAAA.lacBBBB.mncYYY.mccZZZ.gprs

A and B shall be Hex coded digits; Y and Z shall be encoded as single digits (in the range 0-9).

If there are less than 4 significant digits in AAAA or BBBB, one or more "0" digit(s) is/are inserted at the left side to fill the 4 digit coding. If there are only 2 significant digits in YYY, a "0" digit is inserted at the left side to fill the 3 digit coding.

As an example, the logical name for RAC 123A, LAC 234B, MCC 167 and MNC 92 will be coded in the DNS server as:

rac123A.lac234B.mnc092.mcc167.gprs.

The SGSN may then acquire the IP address of the old SGSN from a DNS server, using the logical address. Introducing the DNS concept in GPRS enables operators to use logical names instead of IP addresses when referring to nodes (e.g. GSNs), thus providing flexibility and transparency in addressing. Each PLMN should include at least one DNS server (which may optionally be connected via the DNS service provided by the GSM Association). Note that these DNS servers are GPRS internal entities, unknown outside the GPRS system.

The above implies that at least MCC || MNC || LAC || RAC (= RAI) is sent as the RA parameter over the radio interface when an MS roams to another RA.

If for any reason the new SGSN fails to obtain the address of the old SGSN, the new SGSN takes the same actions as when the corresponding event occurs within one PLMN.

Another way to support seamless inter-PLMN roaming is to store the SGSN IP addresses in the HLR and request them when necessary.

If Intra Domain Connection of RAN Nodes to Multiple CN Nodes (see 3GPP TS 23.236 [23]) is applied then the Network Resource Identifier (NRI) identifies uniquely a given SGSN node out of all the SGSNs serving the same pool area.

If the new SGSN is not able to extract the NRI from the old P-TMSI, it shall retrieve the address of the default SGSN (see 3GPP TS 23.236 [23]) serving the old RA, using the logical name described earlier in this clause. The default SGSN in the old RA relays the GTP signalling to the old SGSN identified by the NRI in the old P-TMSI unless the default SGSN itself is the old SGSN.

If the new SGSN is able to extract the NRI from the old P-TMSI, then it shall attempt to derive the address of the old SGSN from the NRI and the old RAI. NRI-to-SGSN assignments may be either configured (by O&M) in the new SGSN, or retrieved from a DNS server. If a DNS server is used, it shall be queried using the following logical name, derived from the old RAI and NRI information:

nriCCCC.racDDDD.lacEEEE.mncYYY.mccZZZ.gprs

C, D and E shall be Hex coded digits, Y and Z shall be encoded as single digits (in the range 0-9). If there are less than 4 significant digits in CCCC, DDDD or EEEE, one or more "0" digit(s) is/are inserted at the left side to fill the 4 digit coding. If there are only 2 significant digits in YYY, a "0" digit is inserted at the left side to fill the 3 digits coding.

As an example, the logical name for NRI 3A, RAC 123A, LAC 234B, MCC 167 and MNC 92 will be coded in the DNS server as:
nri003A.rac123A.lac234B.mnc092.mcc167.gprs.

If for any reason the new SGSN fails to obtain the address of the old SGSN using this method, then as a fallback method it shall retrieve the address of the default SGSN serving the old RA.

C.2 GPRS Support Nodes

This clause defines a naming convention for GSNs.

It shall be possible to refer to a GSN by a logical name which shall then be translated into a physical IP address. This clause proposes a GSN naming convention which would make it possible for an internal GPRS DNS server to make the translation.

An example of how a logical name of an SGSN could appear is:
sgsnXXXX.mncYYY.mccZZZ.gprs

X, shall be Hex coded digits, Y andZz shall be encoded as single digits (in the range 0-9).

If there are less than 4 significant digits in XXXX one or more "0" digit(s) is/are inserted at the left side to fill the 4 digits coding. If there are only 2 significant digits in YYY, a "0" digit is inserted at the left side to fill the 3 digit coding.

As an example, the logical name for SGSN 1B34, MCC 167 and MNC 92 will be coded in the DNS server as:
sgsn1B34. mnc092.mcc167.gprs

C.3 Target ID

This clause describes a possible way to support SRNS relocation.

In UMTS, when SRNS relocation is executed, a target ID which consists of MCC, MNC and RNC ID is used as routeing information to route to the target RNC via the new SGSN. An old SGSN shall resolve a new SGSN IP address by a target ID to send the Forward Relocation Request message to the new SGSN.

It shall be possible to refer to a target ID by a logical name which shall be translated into an SGSN IP address to take into account inter-PLMN handover. The old SGSN transforms the target ID information into a logical name of the form:

rncXXXX.mncYYY.mccZZZ.gprs

X shall be Hex coded digits; Y and Z shall be encoded as single digits (in the range 0-9). If there are less than 4 significant digits in XXXX, one or more "0" digit(s) is/are inserted at the left side to fill the 4 digits coding. If there are only 2 significant digits in YYY, a "0" digit is inserted at the left side to fill the 3 digit coding. Then, for example, a DNS server is used to translate the logical name to an SGSN IP address.

As an example, the logical name for RNC 1B34, MCC 167 and MNC 92 will be coded in the DNS server as:
rnc1B34.mnc092.mcc167.gprs

Annex D (informative): Applicability and use of the ".3gppnetwork.org" domain name

There currently exists a private IP network between operators to provide connectivity for user transparent services that utilise protocols that rely on IP. This includes (but is not necessarily limited to) such services as GPRS/PS roaming,

WLAN roaming, GPRS/PS inter-PLMN handover and inter-MMSC MM delivery. This inter-PLMN IP backbone network consists of indirect connections using brokers (known as GRXs – GPRS Roaming Exchanges) and direct inter-PLMN connections (e.g. private wire); it is however *not* connected to the Internet. More details can be found in GSMA PRD IR.34 [57].

Within this inter-PLMN IP backbone network, the domain name ".gprs" was originally conceived as the only domain name to be used to enable DNS servers to translate logical names for network nodes to IP addresses (and vice versa). However, after feedback from the Internet Engineering Task Force (IETF) it was identified that use of this domain name has the following drawbacks:

1. Leakage of DNS requests for the ".gprs" top level domain into the public Internet is inevitable at sometime or other, especially as the number of services (and therefore number of nodes) using the inter-PLMN IP backbone increases. In the worst case scenario of faulty clients, the performance of the Internet's root DNS servers would be seriously degraded by having to process requests for a top level domain that does not exist.

2. It would be very difficult for network operators to detect if/when DNS requests for the ".gprs" domain were leaked to the public Internet (and therefore the security policies of the inter-PLMN IP backbone network were breached), because the Internet's root DNS servers would simply return an error message to the sender of the request only.

To address the above, the IETF recommended using a domain name that is *routable* in the pubic domain but which requests to it are not actually *serviced* in the public domain. The domain name ".3gppnetwork.org" was chosen as the new top level domain name to be used (as far as possible) within the inter-PLMN IP backbone network.

Originally, only the DNS servers connected to the inter-PLMN IP backbone network were populated with the correct information needed to service requests for *all* sub-domains of this domain. However, it was later identified that some new services needed their allocated sub-domain(s) to be resolvable by the UE and not just inter-PLMN IP network nodes. To address this, additional, higher-level sub-domains were created:

- "pub.3gppnetwork.org", which is to be used for domain names that need to be resolvable by UEs (and possibly network nodes too) that are connected to a local area network that is connected to the Internet; and

- "ipxuni.3gppnetwork.org", which is to be used for domain names for UNI interfaces that need to be resolvable by UEs that are connected to a local area network that is not connected to the Internet (e.g. local area networks connected to the inter-PLMN IP network of the IPX).

Therefore, DNS requests for the above domain names can be resolved, while requests for all other sub-domains of "3gppnetwork.org" can simply be configured to return the usual DNS error for unknown hosts (thereby avoiding potential extra, redundant load on the Internet's root DNS servers).

The GSM Association is in charge of allocating new sub-domains of the ".3gppnetwork.org" domain name. The procedure for requesting new sub-domains can be found in Annex E.

Annex E (normative): Procedure for sub-domain allocation

When a 3GPP member company identifies the need for a new sub-domain name of ".3gppnetwork.org", that 3GPP member company shall propose a CR to this specification at the earliest available meeting of the responsible working group for this TS. The CR shall propose a new sub-domain name. The new sub-domain proposed shall be formatted in one of the formats as described in the following table.

Sub-domain Format	Intended Usage
<service_id>.mnc<MNC>.mcc<MCC>.3gppnetwork.org (see notes 1 and 2)	Domain name that is to be resolvable by network nodes only. This format inherently adds protection to the identified node, in that attempted DNS resolutions instigated directly from end user equipment will fail indefinitely.
<service_id>.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org (see notes 1 and 2)	Domain name that is to be resolvable by UEs and/or network nodes. This format inherently adds global resolution capability, but at the expense of confidentiality of network topology.
<service_id>.mnc<MNC>.mcc<MCC>.ipxuni.3gppnetwork.org (see notes 1 and 2)	Domain name for UNI interface that is to be resolvable by UEs that are connected to an inter-PLMN IP network that has no connectivity to the Internet. This format inherently adds resolution capability for UEs in closed IP networks e.g. IPX.
<service_id>.mcc<MCC>.visited-country.pub.3gppnetwork.org (see notes 1 and 2)	Domain name in the visited country that is to be resolvable by UEs and/or network nodes, which is not specific to an individual operator.

Table E.1: Sub-domain formats for the "3gppnetwork.org" domain and their respective intended usage

NOTE 1: "<service_ID>" is a chosen label, conformant to DNS naming conventions (usually IETF RFC 1035 [19] and IETF RFC 1123 [20]) that clearly and succinctly describe the service and/or operation that is intended to use this sub-domain.

NOTE 2: "<MNC>" and "<MCC>" are the MNC (padded to the left with a zero, if only a 2-digit MNC) and MCC of a PLMN.

Care should be taken when choosing which format a domain name should use. Once a format has been chosen, the responsible working group shall then check the CR and either endorse it or reject it. If the CR is endorsed, then the responsible working group shall send an LS to the GSMA NG with TSG-CT in copy. The LS shall describe the following key points:

- the context
- the service
- intended use
- involved actors
- proposed new sub-domain name

GSMA NG will then verify the consistence of the proposal and its usage within the domain's structure and interworking rules (e.g. access to the GRX/IPX Root DNS servers). GSMA NG will then endorse or reject the proposal and inform the responsible working group (in 3GPP) and also TSG CT. It is possible that GSMA NG will also specify, changes to the newly proposed sub-domain name (e.g. due to requested sub-domain name already allocated).

NOTE 3: There is no need to request GSMA NG for new labels to the left of an already GSMA NG approved "<service_ID>". It is the responsibility of the responsible working group to ensure uniqueness of such new labels.

It should be noted that services already defined to use the ".gprs" domain name will continue to do so and shall not use the new domain name of ".3gppnetwork.org"; this is to avoid destabilising services that are already live.

Annex F (informative): Change history

Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	New
Apr 1999	GSM 03.03				Transferred to 3GPP CN1	
CN#03	23.003				Approved at CN#03	3.0.0
CN#04	23.003		001		Definition of escape PLMN code	3.1.0
CN#04	23.003		002r1		SSN reallocation for CAP, gsmSCF, SIWF, GGSN, SGSN,	3.1.0
CN#04	23.003		003		Correction of VGC/VBC reference	3.1.0
CN#04	23.003		004		Harmonisation of the MNC-length; correction of CR A019r1	3.1.0
CN#04	23.003		005		Correction to the MNC length	3.1.0
CN#05	23.003		007r1		ASCII coding of <MNC> and <MCC> in APN OI	3.2.0
CN#05	23.003		008		New SSN allocation for RANAP and RNSAP	3.2.0
CN#06	23.003		011		Support of VLR and HLR Data Restoration procedures with LCS	3.3.0
CN#07	23.003		014		Necessity of the function of the calculation of an SGSN IP address from the target ID	3.4.0
CN#07	23.003		016		Definition of Service Area Identification	3.4.0
CN#07	23.003		017r2		Modification of clause 6.2 to enhance IMEI security	3.4.0
CN#07	23.003		018		Coding of a deleted P-TMSI signature	3.4.0
CN#07	23.003		013r2		Introduction of Reserved Service Labels in the APN	3.4.1
CN#08	23.003		019		Missing UTRAN identifiers	3.5.0
CN#08	23.003		021r1		Editorial Modification of clause 6.2.2.	3.5.0
CN#08	23.003		022		IMEI Formats and Encoding	3.5.0
CN#09	23.003		023		Alignment of 23.003 with text from 25.401	3.6.0
CN#10	23.003		024		Moving informative Annex A from 3G TS 29.060 and making it normative.	3.7.0
CN#11	23.003		025		Clarification to Definition of Service Area Identifier	3.8.0
CN#11	23.003		026		Forbidden APN network identifier labels	3.8.0
CN#11	23.003				Updated from R99 to Rel-4 after CN#11	4.0.0
CN#12	23.003		028r1		Remove reference to TS23.022	4.1.0
CN#12	23.003		029r1		New Subsystem Number for the Position Calculation Application Part on the Iupc interface	5.0.0
CN#13	23.003		032		Clarification on APN labels that begin with a digit	5.1.0
CN#13	23.003				Editorial clean up	5.1.0
CN#14	23.003		033		Rules for TMSI partitioning	5.2.0
CN#14	23.003		035		Introduction of Global CN-ID definition	5.2.0
CN#16	23.003		037r1		IuFlex support for determining old SGSN during handover/relocation	5.3.0
CN#16	23.003		038		Allocation of unique prefixes to IPv6 terminals	5.3.0
CN#16	23.003		041r2		Use of a temporary public user identity	5.3.0
CN#16	23.003		044		Restructuring the IMEI to combine the TAC and FAC	5.3.0
CN#16	23.003		045		Use of the TLLI codespace in GERAN Iu mode	5.3.0
CN#17	23.003		048r3		Clarification on the definition of DNS	5.4.0
CN#17	23.003		050r1		Support for Shared Network in connected mode: definition of SNA	5.4.0
CN#17	23.003		053r1		Restructuring the IMEI to combine the TAC and FAC in Annex B	5.4.0
CN#17	23.003		054		SCCP sub-system Number for IM-SSF	5.4.0
CN#18	23.003		055r1		Iur-g Introduction	5.5.0
CN#18	23.003		056r2		Editorial clean-up	5.5.0
CN#18	23.003		057		Correction of the private user identity's form	5.5.0
CN#18	23.003		058		Addition of a reference to the ITU-T RECOMMENDATION E.212 for Mobile Country Codes	5.5.0
CN#18	23.003		059		Correction to the form of public user identity	5.5.0
CN#18	23.003		062		Fix miss-interworking for LMSI handling (LMSI definition)	5.5.0
CN#18	23.003				Corrupted figures 13 – 18 fixed	5.5.1
CN#20	23.003		065		Correction to Annex C.3 – Target ID	5.6.0
CN#21	23.003		072		Correction to definition of Group-ID, Group call area ID and Group Call Reference	5.7.0
CN#21	23.003		073r2		PSI definition	6.0.0
CN#22	23.003		078		On the length of the APN NI	6.1.0
CN#23	23.003		081		Changes and corrections to DNS names	6.2.0

CN#23	23.003		083r2		Changes to enable the GSMA root DNS architecture using ".3gppnetwork.org" TLD	6.2.0
CN#23	23.003		085r1		WLAN access parameters moved from TS 24.234 to TS 23.003	6.2.0
CN#23	23.003		087		Assignment of SSN for Presence Network Agent	6.2.0
CN#24	23.003		086r4		Clarification of the uses of SIP URIs for Public User ID	6.3.0
CN#24	23.003		088r1		Addition of TMGI	6.3.0
CN#25	23.003		089		Background of and procedures for the ".3gppnetwork.org" domain name	6.4.0
CN#25	23.003		090r2		Decorated NAI format	6.4.0
CN#25	23.003		091r1		Introduction of temporary identities	6.4.0
CN#26	23.003		092r2		'otherrealm' format of Decorated NAI	6.5.0
CN#26	23.003		095r1		Clarification of NRI position within (P)-TMSI	6.5.0
CN#26	23.003		096r1		BSF address	6.5.0
CN#27	23.003		097		Clarification of the TMGI	6.6.0
CN#27	23.003		093r3		Definition of Alternative NAI	6.6.0
CT#28	23.003		0099r4		W-APN Definition	6.7.0
CT#28	23.003		0100r5		Correction to wildcards in PSI	6.7.0
					2005-07: Correct line break before clause 14 header	6.7.1
CT#29	23.003		0102r2		Corrections to "3gppnetwork.org" addressing	6.8.0
CT#29	23.003		0103		Addition of addressing for the Generic Access Network	6.8.0
CT#29	23.003		0104r1		PSI routing	6.8.0
CT#31	23.003		0106r1		IETF references update	6.9.0
CT#32	23.003		0107r1		Fast re-authentication identity clarification	6.10.0
CT#32	23.003		0109r1		Case insensitive naming convention	6.10.0
			0111r1		Correction to the W-APN definition	
CT#32	23.003		0112r1		Definition of Anonymous URI in IMS	7.0.0
CT#33	23.003		0117r1		Re-authentication identity definition correction	7.1.0
			0115r3		Definition of MBMS SAI	
CT#34	23.003		0118		Voice Call Continuity Identification and Addressing	7.2.0
			0119r2		Unavailable User Identity	
			0120		Emergency Realm for I-WLAN network advertisment	
			0121		Definition of emergency W-APN	
			0122r2		Format of emergency public identity	
CT#35	23.003		0128r2		Definition of Private Service identity	7.3.0
			0126r2		Definition of emergency APN for IMS em-calls	
			0129r2		Clarification to TMGI definition	
CT#36	23.003		0131r2		Correction of derivation of identifiers, by the UE, using the IMSI	7.4.0
CT#37	23.003		0134r1		Home realm construction for MBMS roaming	7.5.0
			0135r2		PSI clarification	
			0136		Remove emergency APN	
CT#38	23.003		0138		Correction to text describing W-APN format	7.6.0
CT#39	23.003		0141r1		Structure of TMGI	7.7.0
CT#39	23.003		0140		Wildcarded Public User Identities format	8.0.0

CT#40	23.003		0142r2		IMS public and private identity derivation in 3GPP2	8.1.0
			0144		Minor corrections to the IMS clause	
			0146r2		NAI for 3GPP access to Non-3GPP Access Interworking	
			0143r2		Addition of IMS Centralized Services related identities	
CT#41	23.003		0150		Emergency Public User Identity Removal	8.2.0
			0152r3		Introduction of IMC in support of common IMS	
			0153r1		Introduction of STN-SR	
			0154r1		Addition and correction of DNS related identifiers for EPC	
			0155r1		Definition of Globally Unique Temporary UE Identity	
			0156		Reference correction	
			0158r1		Addition of Conference Factory URI for IMS Centralized Services	
			0159r1		Naming for HA discovery HA-APN	
			0160r2		Definition and format of access network identifier	
CT#42	23.003		0161		SGSN related FQDNs	8.3.0
			0162		New "nodes" subdomain for EPC	
			0165		Clarify the mapping between M-TMSI and P-TMSI	
			0166		Revising the GUTI Definition	
			0163r4		Closed Subscriber Group	
			0167r1		Adding the S-TMSI Definition	
			0168r1		Definition of instance Id	
			0169		STN-SR in SGSN	
CT#43	23.003		0170		Correction to NAI format	8.4.0
			0172		Missing service identifiers for DNS procedures	
			0174		Correction of the GUTI format	
			0176r1		Correction of the GUTI P-TMSI mapping	
			0177		Corrections to Service Continuity addressing	
			0178r1		Support of EAP-AKA'	
			0179r2		Naming for ANDSF discovery	
			0180r1		ePDG naming	
			0181r2		Clarification about canonical form of IMS Public User Identity when format is TEL URL	
			0182		Temporary Identity Tag Values for Fast Re-authentication Ids	
			0187r2		DNS-APN-OI	
CT#44	23.003		0189r1		HNB Name Definition	8.5.0
			0190r1		Clarification on TAI FQDN	
			0191		Service Parameters for S2c	
			0193r2		Reference update for draft-montemurro-gsma-imei-urn	
CT#45	23.003		0194r1		Public User Identity definition in TS 23.003	8.6.0
			0197r1		Inclusion of CSG Type	
CT#45	23.003		0199r1		IMEI Based NAI definitions for emergency services	9.0.0

CT#46	23.003		0200r 1		IMEI based NAI	9.1.0
			0205r 4		IMEI Based NAI	
			0210r 1		Reintroducing Emergency APN definition for IMS based Emergency Call	
			0212r 1		Clarification for the format of ANDSF-SN in roaming scenario	
			0215		Tracking Area Code	
			0217		E-UTRAN Cell Global Identification definition	
CT#47	23.003		0213r 4		Defining H(e)NB identity	9.2.0
			0219r 2		Exclude prepended digit from the NAI in PMIPv6	
			0221r 2		APN-FQDN construction	
			0223		Corrections to APN structure	
			0225r 1		Correction on Home Network Realm/Domain	
			0227		Corrections to IMS Public Identity	
CT#48	23.003		0229r 1		Removal of the redundancy reference to 23.401	9.3.0
			0232r 1		IMEI and IMEISV	
			0235r 1		Remove ambiguities and improved definition of HNB Unique Identity	
			0237r 2		Essential corrections to GUTI mapping	
CT#49	23.003		0242r 1		PSI use for services hosted in an AS	9.4.0
			0246r 3		Essential corrections to GUTI mapping	
			0247r 2		Use of NRI	
			0256		Format of the Unavailable User Identity	
			0257		Clarification of UE behaviour with regards to LAC format	
CT#50	23.003		0252r 2		Correction of C-MSISDN definition	9.5.0
			0265		Updating IMEI URN draft reference	
			0268r 1		Determination of type of source node during TAU/RAU	
CT#50	23.003		0258r 3		eNodeB-ID FQDN for DNS procedures	10.0.0
			0269r 1		Determination of type of source node during TAU/RAU	
			0259		Service Parameter on PGW selection for GTP based S2b	
CT#51	23.003		0274r 3		Relay Node OAM system identification	10.1.0
			0279r 3		Correction of C-MSISDN definition	
			0277r 1		Determination of type of source node during TAU/RAU	
			0285		Correction to a reference of an outdated IETF draft to an RFC	
			0280r 2		Correction to the reserved values for Tracking Area Code (TAC)	
			0286		DNS Service Support For Sv	
			0289		Clarfication of decoding of NRI	
CT#52	23.003		0290		Closed Subscriber Group clarification	10.2.0
			0293r 2		UE moving from E-UTRAN to GERAN	
			0294r 2		XCAP Addressing	

			0296r1		APN Network Identifier	
			0299		Updating IMEI URN draft reference	
CT#53	23.003		0307		Updating IMEI URN draft reference	10.3.0
			0282r4		Format of Public User Identities and SIP/TEL URI	
			0303r3		Emergency NAI for UICC-less Terminal	
CT#54	23.003		0316r1		Definition of Distinct Public User Identity	10.4.0
			0309r1		Emergency NAI for UICC-less Terminal	
CT#54	23.003		0308r2		APN Operator Identifier for local breakout	11.0.0
			0312r2		Definition of STI-rSR	
CT#55	23.003		0334		BSF address correction	11.1.0
			0322r2		Correction to domain name for XCAP Root URI	
			0325		Updating IMEI URN draft reference	
			0317r2		Clarification of GUTI mapping	
			0318		Service Parameter on PGW selection for GTP based S2a	
CT#56	23.003		0320r6		MTC External Identifier	11.2.0
			0337r1		New Service Parameters for CS to PS SRVCC	
			0319r5		Definition of A-MSISDN	
			0335r2		MME Number for SMS in MME	
			0311r7		SSN Reallocation for CSS and its Number Definition	
CT#57	23.003		0338r1		External Identifier definition	11.3.0
			0339r1		PS only subscription w/o MSISDN	
			0340r1		NCC allocation in a shared network	
			0342r1		MSB in the GUTI and P-TMSI mapping	
			0345r2		Clarification to MME FQDN	
CT#58	23.003		0347		Clarification on the use of APN Operator Identifier	11.4.0
			0348r1		PS only subscription without MSISDN	
			0352r1		Updating IMEI URN draft reference	
CT#59	23.003		0346r5		MME FQDN Clarification	11.5.0
CT#61	23.003		0358		Updating IMEI URN draft reference	11.6.0
			0361r1		MBMS SAI Definition Correction for LTE Access	
			0363r2		NRI and MMEC coordination	
CT#61	23.003		0362r2		SIPTO permission for Local Network LHN ID definition	12.0.0
			0364		GERAN Iu Mode	12.0.0
CT#62	23.003		0370		Updating IMEI URN draft reference	12.1.0
			0365r3		Multi-Vendor eNB Plug and Play	12.1.0
CT#63	23.003		0379		Updating IMEI URN draft reference	12.2.0
			0371r2		Update of working procedures with GSMA IREG	12.2.0

			0372r1		TWAN Operator Name	12.2.0
CT#64	23.003		0381r4		Addition of ProSe Application ID format	12.3.0
			0382r5		Addition of ProSe Application Code format	12.3.0
			0383r1		Correct definition of Decorated NAI for Evolved Packet Core (EPC)	12.3.0
			0384r1		Definition of Alternative NAI for Evolved Packet Core (EPC)	12.3.0
			0386r6		Conference Factory URI for IMS	12.3.0
07-2014	23.003				Clause 19.3.7 title corrected	12.3.1
CT#65	23.003		0391		Updating IMEI URN draft reference to RFC 7254	12.4.0
			0392r2		Identification of the HSS	12.4.0
			0393r2		Update of ProSe Application Code format	12.4.0
			0394		IMSI based Decorated NAI	12.4.0
10-2014	23.003				Clause number 10.2.2 added.	12.4.1
CT#66	23.003		0398r1		Clarification of NAI handling	12.5.0
			0399r2		Maintenance of I-WLAN requirements	12.5.0
			0402		Addressing and Identifications for Bootstrapping MBMS Service Announcement	12.5.0
			0401r1		Definiton for EPC Prose User ID	12.5.0
			0403r1		Prose Application ID Name description	12.5.0
CT#66	23.003		0396r3		Defining app protocol name for Nq and Nq'	13.0.0
CT#67	23.003		0409r2		Extension of decorated NAI	13.1.0
			0414		Definition of Vendor ID	13.1.0
			0413r2		Clarification in the definition of the ProSe Application Code	13.1.0
CT#68	23.003		0412r6		Clarification of Root NAI and Decorated NAI	13.2.0
			0416r1		Correction of examples for the Fast-Reauth NAI	13.2.0
			0417r1		Domain name starting by a digit	13.2.0
CT#69	23.003		0420		Removal of Editor's Note about ProSe Application Code Length	13.3.0
			0418r3		Definition of IMSI-Group Identifier	13.3.0
			0421r1		FQDN format for ProSe Function	13.3.0
CT#70	23.003		0423r2		FQDN for ePDG selection for emergency bearer services	13.4.0
			0424r1		FQDN for ePDG selection (for non-emergency bearer services)	13.4.0
			0431r4		Introduce home network domain name for OCS	13.4.0
			0426r2		ProSe Application code and Metadata index	13.4.0
			0427r1		ProSe identifiers for restricted ProSe direct discovery	13.4.0
			0433r1		ProSe identifiers used in direct discovery for public safety	13.4.0
			0429r1		Presence Reporting Area Identifier	13.4.0
			0432r2		Enhancement of service parameters to support Decor	13.4.0

CT#71	23.003		0434r1		Addition of ProSe Application Code Prefix and ProSe Application Code Suffix formats	13.5.0
			0437r1		ePDG selection with DNS-based Discovery of Regulatory Requirements	13.5.0
			0438r1		Clarification of TAC Allocation	13.5.0
2016-06	CT#72	CP-160237	0441	1	Replacement field used in DNS-based Discovery of regulatory requirements	13.6.0
2016-06	CT#72	CP-160237	0441	1	Replacement field used in DNS-based Discovery of regulatory requirements	13.6.0
2016-06	CT#72	CP-160219	0439	3	Clarification on the construction of the private user identity	14.0.0
2016-09	CT#73	CP-160425	0443	1	Domain Name for MCPTT confidentiality protection	14.1.0
2016-09	CT#73	CP-160417	0445	-	Update of definition of BSIC to include Radio frequency Colour Code	14.1.0
2016-12	CT#74	CP-160679	0448	1	FQDNs for ePDG selection for Emergency services	14.2.0
2016-12	CT#74	CP-160679	0449	1	NAI for Emergency services for UEs without IMSI or with unauthenticated IMSI	14.2.0
2016-12	CT#74	CP-160672	0456	1	Unknown User Identity	14.2.0
2016-12	CT#74	CP-160666	0458	1	IMSI-Group-Id	14.2.0
2016-12	CT#74	CP-160781	0459	3	KeyName-NAI format	14.2.0
2017-03	CT#75	CP-170042	0447	4	DCN Identifier	14.3.0
2017-03	CT#75	CP-170045	0460	-	Mission Critical Services	14.3.0
2017-06	CT#76	CP-171016	0464	1	Add an explicit reference to TS33.234 and TS24.234	14.4.0
2017-06	CT#76	CP-171033	0465	2	FQDN for DNS Query of Local Emergency Numbers	14.4.0
2017-06	CT#76	CP-171033	0466	1	NAI for emergency services over WLAN access to EPC	14.4.0
2017-06	CT#76	CP-171032	0467	1	Addition of V2X Control Function FQDN format	14.4.0
2017-06	CT#76	CP-171029	0470	1	External Group Identifier	14.4.0
2017-06	CT#76	CP-171036	0471	2	Sx Service Parameters	14.4.0
2017-06	CT#76	CP-171031	0472	1	Reserved range of TMGI for Receive Only Mode	14.4.0
2017-06	CT#76	CP-171040	0468	1	External Identifier on Sh	15.0.0
2017-09	CT#77	CP-172015	0475	-	PGW selection for WLAN with deployed DCNs	15.1.0
2017-09	CT#77	CP-172024	0476	1	WebRTC Web Server Function discovery	15.1.0
2017-12	CT#78	CP-173034	0479	1	N3IWF FQDN	15.2.0
2017-12	CT#78	CP-173034	0480	1	Definition of 5G-GUTI and mapping between 5G-GUTI and EPS GUTI	15.2.0
2017-12	CT#78	CP-173034	0485	1	Introducing the S-NSSAI definition	15.2.0
2017-12	CT#78	CP-173036	0482	1	SGW/PGW selection for NR	15.2.0
2017-12	CT#78	CP-173022	0484	2	Align emergency number FQDN and Replacement field with procedures in TS 24.302	15.2.0
2017-12	CT#78	CP-173024	0486	2	IMEI based SIP URI for P-Preferred-Identity	15.2.0
2018-03	CT#79	CP-180017	0488	-	Specifying the length of the sub-label of the Country based Emergency Numbers FQDN	15.3.0
2018-03	CT#79	CP-180024	0489	1	Definition of Service ID for WLAN based ProSe Direct Discovery	15.3.0
2018-03	CT#79	CP-180022	0490	2	Rename entity that do national allocation/assignment of numbering/addressing/identification resources	15.3.0
2018-03	CT#79	CP-180022	0491	2	Correct parts concerning ITU-T Rec. E.212 that is not correct in TS 23.003	15.3.0
2018-03	CT#79	CP-180022	0492	2	Change terminology from ISDN number/ISDN numbering plan to E.164 number and E.164 numbering plan and adjust abbreviation of MSISDN	15.3.0
2018-03	CT#79	CP-180026	0494	1	Definition of NCI and NCGI	15.3.0
2018-03	CT#79	CP-180026	0498	1	External identifier in 5G	15.3.0
2018-06	CT#80	CP-181132	0497	4	NF Service Endpoint Format for Inter PLMN Routing	15.4.0
2018-06	CT#80	CP-181132	0500	2	NRF FQDN specification for NRF discoverability	15.4.0
2018-06	CT#80	CP-181132	0501	2	NSSF FDQN for NSSF discovery before NRF is queried	15.4.0
2018-06	CT#80	CP-181132	0502	1	AMF Name	15.4.0
2018-06	CT#80	CP-181132	0504	2	Structure of SUPI and SUCI	15.4.0
2018-06	CT#80	CP-181132	0505	1	GUAMI	15.4.0
2018-06	CT#80	CP-181132	0508	2	Definition of DNN	15.4.0
2018-06	CT#80	CP-181182	0503	2	Changed length and mapping of 5GS Temporary Identifiers	15.4.0
2018-09	CT#81	CP-182084	0509	5	TAI in 5GC	15.5.0
2018-09	CT#81	CP-182084	0511	3	SST value not associated with any valid SD	15.5.0

2018-09	CT#81	CP-182084	0512	3	Definition of PEI	15.5.0
2018-09	CT#81	CP-182084	0514	1	5GS TAI FQDN	15.5.0
2018-09	CT#81	CP-182084	0515	-	5GS Tracking Area Identity based ePDG FQDN	15.5.0
2018-09	CT#81	CP-182084	0516	1	SUPI definition and NAI format	15.5.0
2018-09	CT#81	CP-182084	0517	4	SUCI definition and NAI format	15.5.0
2018-09	CT#81	CP-182084	0518	1	Network Capability SMF	15.5.0
2018-09	CT#81	CP-182084	0519	1	AMF Discovery by 5G-AN	15.5.0
2018-09	CT#81	CP-182067	0510	1	DNS records for selecting a node with a network capability in a Dedicated Core Network	15.5.0
2018-12	CT#82	CP-183092	0529	3	SUCI definition and NAI format	15.6.0
2018-12	CT#82	CP-183092	0520	1	Internal-Group Identifier	15.6.0
2018-12	CT#82	CP-183092	0521	1	Definition of GPSI	15.6.0
2018-12	CT#82	CP-183092	0522	-	Selection of a PGW-U/UPF	15.6.0
2018-12	CT#82	CP-183092	0523	1	Correct missing 5GC NAI	15.6.0
2018-12	CT#82	CP-183092	0524	2	Telescopic FQDN	15.6.0
2018-12	CT#82	CP-183092	0525	1	Clarification of MSIN in SUCI	15.6.0
2018-12	CT#82	CP-183092	0526	-	Routing ID	15.6.0
2018-12	CT#82	CP-183092	0527	1	SUPI definition	15.6.0
2018-12	CT#82	CP-183092	0528	-	EPS interworking with 5GS	15.6.0
2019-06	CT#84	CP-191058	0530	1	Derivation of SUPI from SUCI	15.7.0
2019-06	CT#84	CP-191058	0533	-	NRF and NSSF URIs	15.7.0
2019-09	CT#85	CP-182116	0541	-	Presence Reporting Area Identifier (PRA ID) in 5GS	15.8.0
2019-09	CT#85	CP-182232	0540	3	Clarification about the Routing Indicator	15.8.0
2019-09	CT#85	CP-192133	0534	-	Closed Access Group	16.0.0
2019-09	CT#85	CP-192133	0539	2	Network Identifier for SNPN	16.0.0
2019-09	CT#85	CP-192189	0543	1	UE radio capability ID format	16.0.0
2019-09	CT#85	CP-192194	0536	2	Definition of NF Set ID	16.0.0
2019-09	CT#85	CP-192194	0537	1	Definition of NF Service Set ID	16.0.0
2019-09	CT#85	CP-192194	0538	1	Definition of SMF Set FQDN	16.0.0

3GPP TS 23.012 V15.0.0 (2018-06)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Location management procedures (Release 15)

Keywords
GSM, UMTS, network, location, management

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Specification (TS) has been produced by the 3rd Generation Partnership Project (3GPP).

The present document defines the location management procedures within the 3GPP system.

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document describes the location management procedures for the circuit switched domain, with respect to the application level functional behaviour. This is to be distinguished from the corresponding protocol handling behaviour, which is specified in 3GPP TS 29.002 [8]. The following location management procedures are included:

- location updating;
- location cancellation;
- MS purging;
- IMSI attach/detach.

The procedures in the Mobile Station (MS) are described in 3GPP TS 23.022 [6]. The procedures between MSC, VLR and HLR utilise the Mobile Application Part (MAP) and details concerning the protocol handling are contained in 3GPP TS 29.002 [8].

The present document excludes location management procedures for the packet switched domain, which are covered in 3GPP TS 23.060 [20].

The descriptions herein depict a logical separation between the MSC and VLR. This logical separation, as well as the messages transferred between the two logical entities are the basis of a model used to define the externally visible behaviour of the MSC/VLR, which a may be a single physical entity. They do not impose any requirement except the definition of the externally visible behaviour.

1.1 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TR 21.905: "3G Vocabulary".

[2] 3GPP TS 23.002: "Network architecture".

[3] 3GPP TS 23.003: "Numbering, addressing and identification".

[4] 3GPP TS 23.007: "Restoration procedures".

[5] 3GPP TS 23.008: "Organization of subscriber data".

[5a] 3GPP TS 23.018: "Basic call handling; Technical realization".

[6] 3GPP TS 23.022: "Functions related to Mobile Station (MS) in idle mode".

[7] 3GPP TS 23.116: "Super-Charger Technical Realisation; Stage 2".

[8] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[9] 3GPP TS 29.007: "General requirements on interworking between the Public Land Mobile Network (PLMN) and the Integrated Services Digital Network (ISDN) or Public Switched Telephone Network (PSTN)".

[10] 3GPP TS 43.020: "Security related network functions".

[11] 3GPP TS 23.078: " Customised Applications for Mobile network Enhanced Logic (CAMEL) Phase 4 – stage2".

[11a] 3GPP TS 23.195: "Provision of UE Specific Behaviour Information to Network Entities".

[12] 3GPP TS 23.236: "Intra Domain Connection of RAN Nodes to Multiple CN Nodes".

[13] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols - Stage 3".

[14] 3GPP TS 29.010: "Information element mapping between Mobile Station - Base Station System and BSS - Mobile-services Switching Centre (MS - BSS - MSC) Signalling procedures and the Mobile Application Part (MAP)".

[15] 3GPP TS 32.422: "Subscriber and equipment trace: Trace control and configuration management".

[16] 3GPP TS 32.421: "Subscriber and equipment trace: Trace concepts and requirements".

[17] 3GPP TS 25.413: "UTRAN Iu interface RANAP signalling".

[18] 3GPP TR 29.994: "Recommended infrastructure measures to overcome specific Mobile Station (MS) faults".

[19] 3GPP TS 24.368: "Non-Access Stratum (NAS) configuration Management Object (MO)".

[20] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

1.2 Abbreviations

Abbreviations are listed in 3GPP TR 21.905 [1].

In addition, for the purposes of the present document, the following abbreviations apply:

ADD	Automatic Device Detection
CSG	Closed Subscriber Group
CSS	CSG Subscriber Server
PUESBINE	Provision of User Equipment Specific Behaviour Information to Network Entities
UESBI-Iu	User Equipment Specific Behaviour Information over the Iu interface

2 Definitions

2.1 Location management

Location management means that the PLMNs keep track of where the MSs are located in the system area. The location information for each MS is stored in functional units called location registers. Functionally, there are two types of location registers:

- the Home Location Register where all subscriber parameters of an MS are permanently stored, and where the current location may be stored;
- the Visitor Location Register where all relevant data concerning an MS are stored as long as the station is within the area controlled by that visitor location register;
- the CSG Subscriber Server where the CSG subscription data are stored in the visited PLMN for inbound roaming MS, and where the current location may be stored.

See also 3GPP TS 23.002 [2] where the network architecture is described, and 3GPP TS 23.008 [5] where the data stored in the location registers are described.

The action taken by a MS in order to provide location information to the PLMN will be referred to as location updating.

2.2 Location area and MSC area

The MSC area is composed of the area covered by all base stations controlled by the MSC. An MSC area may consist of several location areas. A location area is an area in which, after having performed a location update once, MSs may roam without being required to perform subsequent location updates for reason of location change. A location area consists of one or more cells.

For further details of the network architecture, see 3GPP TS 23.002 [2].

2.3 Location area identification

The Location Area Identification (LAI) plan is part of the base station identification plan. The base stations are identified uniquely (see 3GPP TS 23.003 [3]).

2.4 IMSI detach/attach operation

The support of IMSI detach/attach operation is mandatory in MSs. The facility is optional in the fixed infrastructure of the PLMN.

2.4.1 Explicit IMSI detach/attach

Explicit IMSI detach operation is the action taken by an MS to indicate to the PLMN that the station has entered an inactive state (e.g. the station is powered down). Explicit IMSI attach operation is the action taken by an MS to indicate that the station has re-entered an active state (e.g. the station is powered up).

2.4.2 Implicit IMSI detach

Implicit IMSI detach operation is the action taken by the VLR to mark an MS as detached when there has been no successful contact between the MS and the network for a time determined by the implicit detach timer. The value of the implicit detach timer is derived from the periodic location updating timer; when the MSC/VLR applies Mobility Management Congestion Control to a MS, the MSC/VLR may need to adjust the Implicit Detach timer as specified in clause 3.7.2. During an established radio contact, the implicit detach timer shall be prevented from triggering implicit detach. At the release of the radio connection, the implicit detach timer shall be reset and restarted. Implicit IMSI detach shall also be performed in the case of a negative response to an IMEI check.

2.5 Use of the term mobile station (MS) in the present document

In order to simplify the text the term Mobile Station (MS) as used in relation to location management refers to the entity where the IMSI is stored, i.e., in card operated MSs the term Mobile Station (MS) refers to the card.

2.6 Paging area

As an option, and for paging optimization purpose, the VLR may control Paging Areas. A Paging Area (PgA) is composed of up to 5 Location Areas, and the MSC area is composed of several Paging Areas. Paging areas may overlap each other. The Paging Area is stored in the HLR and updated at each paging area change. The Paging Area is sent by the HLR to the VLR at roaming number request and may be used by the MSC/VLR for paging (e.g. when LAI is not known, after MSC/VLR restart) (see 3GPP TS 23.018 [5a]).

3 General procedures in the network related to Location Management

3.1 Procedures in the MSC related to Location Updating

The MSC shall pass messages related to location updating between the MS and the VLR.

3.2 Procedures in the VLR related to Location Updating

FFS

3.3 Procedures in the HLR related to Location Updating

FFS

3.4 Normal Location Updating and IMSI detach/attach operation

When receiving a Location Updating Request or an IMSI detach/attach message from an MS, the MSC shall convey the message to its associated Visitor Location Register. Any response from the location register shall similarly be conveyed to the MS.

3.5 IMSI enquiry procedure

The MS shall identify itself by either the IMSI or the TMSI plus Location Area Identification of the previous VLR. In the latter case the new VLR shall attempt to request the IMSI and authentication parameters from the previous VLR by the methods defined in 3GPP TS 29.002 [8].

If this procedure fails, or if the TMSI is not allocated, the VLR shall request that the MS identifies itself by use of the IMSI.

3.6 Information transfer between Visitor and Home Location Registers

3.6.1 Procedures for location management

Detailed procedures for exchange of and location updating information between visitor and home location registers are given in 3GPP TS 29.002 [8]. Below follows an overview of these procedures.

3.6.1.1 Location updating procedure

This procedure is used when an MS registers with a Visitor Location Register.

The VLR provides its address to the HLR.

The VLR may also allocate an optional identity for the MS at location updating: the Local Mobile Station Identity (see 3GPP TS 23.003 [3]).

3.6.1.2 Downloading of subscriber parameters to the VLR

As a part of the location updating procedure, the Home Location Register will convey the subscriber parameters of the MS which need to be known by the visitor location register for proper call handling. This procedure is also used

whenever there is a change in the subscriber parameters that need to be conveyed to the VLR (e.g. change in subscription, a change in supplementary services activation status).

If the HPLMN applies the multinumbering option, different MSISDNs are allocated for different Basic Services (see 3GPP TS 29.007 [9]) and stored in the HLR. Among these MSISDNs, the Basic MSISDN Indicator as part of the HLR subscriber data (see 3GPP TS 23.008 [5]) marks the 'Basic MSISDN' to be sent to the VLR at location update. It is used in the VLR for call handling as calling party and as line identity.

If the HPLMN applies the Administrative Restriction of Subscribers' Access feature, the HLR shall convey the subscriber access restriction parameter (AccessRestrictionData) to the VLR. The VLR shall check this subscription parameter against the radio access technology that supports the LA/RA in which the UE is roaming to decide whether the location update should be allowed or rejected.

For further information of the Subscriber access restriction see 3GPP TS 23.008[5].

3.6.1.3 Location cancellation procedure

The procedure is used by the home location register to remove a MS from a visitor location register. The procedure will normally be used when the MS has moved to an area controlled by a different location register. The procedure can also be used in other cases, e.g. an MS ceases to be a subscriber of the Home PLMN.

3.6.1.4 Mobile subscriber purging procedure

A VLR may purge the subscriber data for an MS which has not established radio contact for a period determined by the network operator. Purging means to delete the subscriber data and to "freeze" the TMSI that has been allocated to the purged MS in order to avoid double TMSI allocation. The VLR shall inform the HLR of the purging.

When the HLR is informed of the purging, it shall set the flag "MS purged" in the IMSI record of the MS concerned. Presence of the "MS purged" flag will cause any request for routing information for a call or short message to the MS to be treated as if the MS were not reachable.

In the VLR, the "frozen" TMSI is freed for usage in the TMSI allocation procedure by location updating for the purged MS in the same VLR, location cancellation for the purged MS or, in exceptional cases, by O&M.

In the HLR, the "MS purged" flag is reset by the location updating procedure and after reload of data from the non-volatile back-up that is performed when the HLR restarts after a failure.

3.6.1.5 Support for subscription without MSISDN

An MSC/VLR may support delivery of SMS destined to an MS without MSISDN for GPRS and EPS operation whereby a MSISDN is not allocated as part of the subscription data (see 3GPP TS 23.060 [3] subclause 5.3.17 and 3GPP TS 23.401 [72]).

An MSC/VLR which supports MSISDN-less operation shall indicate such support to the HLR in the MAP Update Location request.

The HLR should reject a MAP Update Location request received for an MSISDN-less subscription from a VLR not indicating support of MSISDN-less operation, with a cause indicating that roaming is not allowed.

The HLR shall download the subscriber parameters to the VLR as per subclause 3.6.1.2 but without an MSISDN for an MSISDN-less subscription if the VLR indicates support of MSISDN-less operation.

NOTE 1: VLRs not supporting MSISDN-less operation can face unpredictable problems if the HLR was downloading subscriber parameters without an MSISDN or with a dummy MSISDN shared across multiple subscriptions.

NOTE 2: Some services have unresolved MSISDN dependencies and are not supported at operation without MSISDN. See 3GPP TS 23.060 [3] subclause 5.3.17.

NOTE 3: The HLR can accept a MAP Update Location request received for an MSISDN-less subscription from a VLR not indicating support of MSISDN-less operation if the HLR knows by proprietary means that the VLR supports MSISDN-less operation in a proprietary way (e.g. with a dummy MSISDN value).

3.7 Overload Protection

3.7.1 Overview

As the number of mobile devices increase and become more automated (Machine Type Communication, MTC type devices) the network is at greater risk of becoming overloaded. Additional mechanisms may be deployed to prevent and or control overload and congestion. This sub-clause describes such optional mechanisms.

The succeeding descriptions applies to Network Mode of Operation II (requesting CS only). For NMO I (requesting both CS and PS) the procedures are described in 3GPP TS 23.060 [20].

3.7.2 Congestion Control during Mobility Management

The MSC or VLR may support the capability to reject Location Updating Requests or IMSI Attach messages from an MS if the node is experiencing congestion.

The MSC/VLR may indicate the rejection is due to congestion with a specific congestion cause value and a specific back-off timer, see 3GPP TS 24.008 [13].

The Mobility Management back-off timer shall not impact Cell/RAT and PLMN change. Cell/RAT and RA change do not stop the Mobility Management back-off timer. The Mobility Management back-off timer shall not be a trigger for PLMN reselection. The back-off timer is stopped as defined in 3GPP TS 24.008 [13] when a new PLMN that is not an equivalent PLMN is accessed.

While the Mobility Management back-off timer is running, the MS shall not initiate any Mobility Management procedures. However, the MS is allowed to initiate Mobility Management procedures for priority/emergency services and mobile terminated services even when the Mobility Management back-off timer is running.

If the MS receives a paging request from the MSC/VLR while the Mobility Management back-off timer is running, the MS shall stop the Mobility Management back-off timer and initiate the CM Service Request procedure.To avoid that large amounts of MSs initiate deferred requests (almost) simultaneously, the MSC/VLR should select the Mobility Management back-off timer value so that deferred requests are not synchronised.

The decision to apply congestion control is made by the MSC/VLR, the detailed criteria for which is outside the scope of this specification but may for example take into account the low access priority indication if signalled by MSs.

The MSC/VLR should use implicit detach timer values that are larger than the Mobility Management back-off timer values to avoid that the MSC/VLR implicitly detaches the MS before the MS has performed a LAU procedure, which could lead to unneccessary signalling after the back-off timer expires.

3.7.3 Extended periodic LAU Signalling

To reduce network load from periodic location updating (LAU) signalling and to increase the time until the MS detects a potential need for changing the RAT or PLMN (e.g. due to network problems) longer values of the periodic LAU timer and implicit detach timer should be supported.

A long periodic LAU timer value may be locally configured at the MSC/VLR for MS configured for low access priority (see 3GPP TS 24.368 [19]) or may be stored as part of the subscription data in the HLR. During the IMSI Attach and Location Updating procedures, the MSC/VLR should allocate the periodic LAU timer value for the MS based on VPLMN operator policy, low access priority indication from the MS, and subscription information received from the HSS. If the allocated periodic LAU timer value is longer than T3212, the MSC/VLR shall provide the MS with the periodic LAU timer in the Location Updating Accept message as specified in 3GPP TS 24.008 [13].

If the subscriber is not roaming and the MSC/VLR receives a subscribed periodic LAU timer value from the HSS, it should allocate the subscribed value to the MS as periodic LAU timer. If the subscriber is roaming and the MSC/VLR receives a subscribed periodic LAU timer value from the HSS, the MSC/VLR may use the subscribed periodic LAU timer value as an indication to decide for allocating a locally configured periodic LAU timer value to the MS.

3.8 Information transfer between VLR and CSG Subscriber Server

3.8.1 Procedures for location management

3.8.1.1 General

Detailed procedures for exchange of and location updating information between VLR and CSG Subscriber Server are given in 3GPP TS 29.002[8]. This clause follows an overview of these procedures.

3.8.1.2 Updating VCSG Location procedure

This procedure is used when an MS registers with a Visitor Location Register and there is a need to do a registration with the CSS.

The VLR provides its address to the CSS.

3.8.1.3 Downloading of VPLMN CSG subscription data to the VLR

As a part of the location updating procedure, the CSG Subscriber Server shall convey the VPLMN CSG subscription data of the roaming MS which needs to be known by the visitor location register for determine whether the MS can access the current cell to have CS services. This procedure is also used whenever there is a change in the VPLMN CSG subscription data that needs to be conveyed to the VLR.

3.8.1.4 VCSG Location cancellation procedure

The procedure is used by the CSS to remove a MS from a CSS. The procedure will normally be used when there is a removal of the CSG subscription data in CSS and of the MS registration including the case where a MS was registered in CSS but without CSG data.

4 Detailed Procedures in the network related to Location Management

The text in this clause is a supplement to the definition in the SDL diagrams; it does not duplicate the information in the SDL diagrams.

This specification shows the location management application processes interworking with the MAP protocol handler, which is specified in 3GPP TS 29.002 [8]. The MAP protocol defines supervision timers. If a supervision timer expires before a distant entity responds to a signal, the handling is as defined in 3GPP TS 29.002 [8]. In general, the protocol handler reports timer expiry to the application as an error condition or negative response. Where a timer is shown in this specification, therefore, it is an **application timer** rather than a **protocol** timer. Interworking with the protocol handlers uses functional signal names which do not necessarily have a one-to-one correspondence with the names of messages used in the MAP protocols.

4.1 Location Updating

4.1.1 Detailed procedure in the MSC

4.1.1.1 Process Update_Location_Area_MSC

Sheet 1: Location Update corresponds to a Location_Registration_Request indicating any of the following:

- Normal location update;

- Periodic location update;
- IMSI attach.

Sheet 1: The procedures Check_IMEI_MSC, Obtain_IMEI_MSC and Obtain_IMSI_MSC are specified in 3GPP TS 23.018 [5a].

Sheet 1: The input signal "Send UESBI-Iu to Access Network" carries the IMEISV.

Sheet 1: The task "Convert IMEISV to UESBI" is defined in 3GPP TS 23.195 [11a].

Sheet 2: The procedure Check_IMEI_MSC is specified in 3GPP TS 23.018 [5a].

Sheet 2: When the MSC receives a Set Ciphering Mode request from the VLR, it sends a Start ciphering request towards the MS. After that, the Forward new TMSI and Update Location Area ack may be received in any order.

Sheet 2: The Forward new TMSI may also be received prior to Update Location Area negative response if the option "TMSI reallocation in case of Location Update reject with cause #13 (roaming not allowed in Location Area) or #15 (no suitable cells in Location Area)" is applicable (see §4.1.2.3). The new TMSI is forwarded together with the new LAI. They are kept in the UE/SIM on receipt of the Location Update reject with cause #13 or #15 (see 3GPP TS 24.008 [13]).

Sheet 2: IMEISV trace list shall be made available to the MSC. The list may contain IMEISV entries if Management Based Trace Activation is supported in RAN and MSC has received the trace list in the Uplink Information Transfer message (See 3GPP TS 32.422 [15] and 25.413 [17]). The test "Current IMEISV included in IMEISV trace list?" will follow the "no" case when no entries exist.

Sheet 2: For Trace Invocation in RAN concepts and procedures see 3GPP TSs 32.421 [16], 32.422[15] and 25.413[17].

Sheet 2: IMEISV trace list

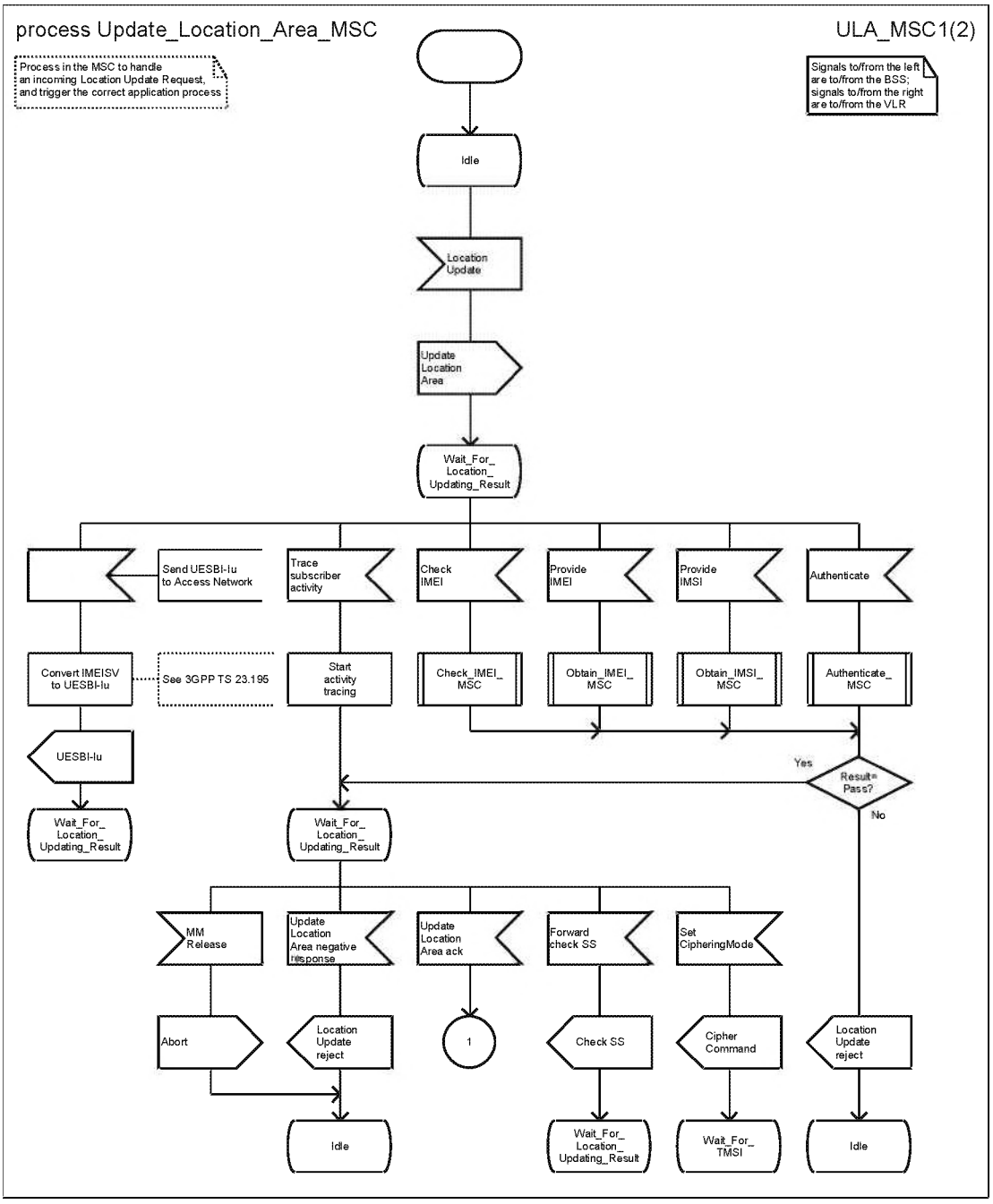

Figure 4.1.1.1 (sheet 1 of 2): Process Update_Location_Area_MSC

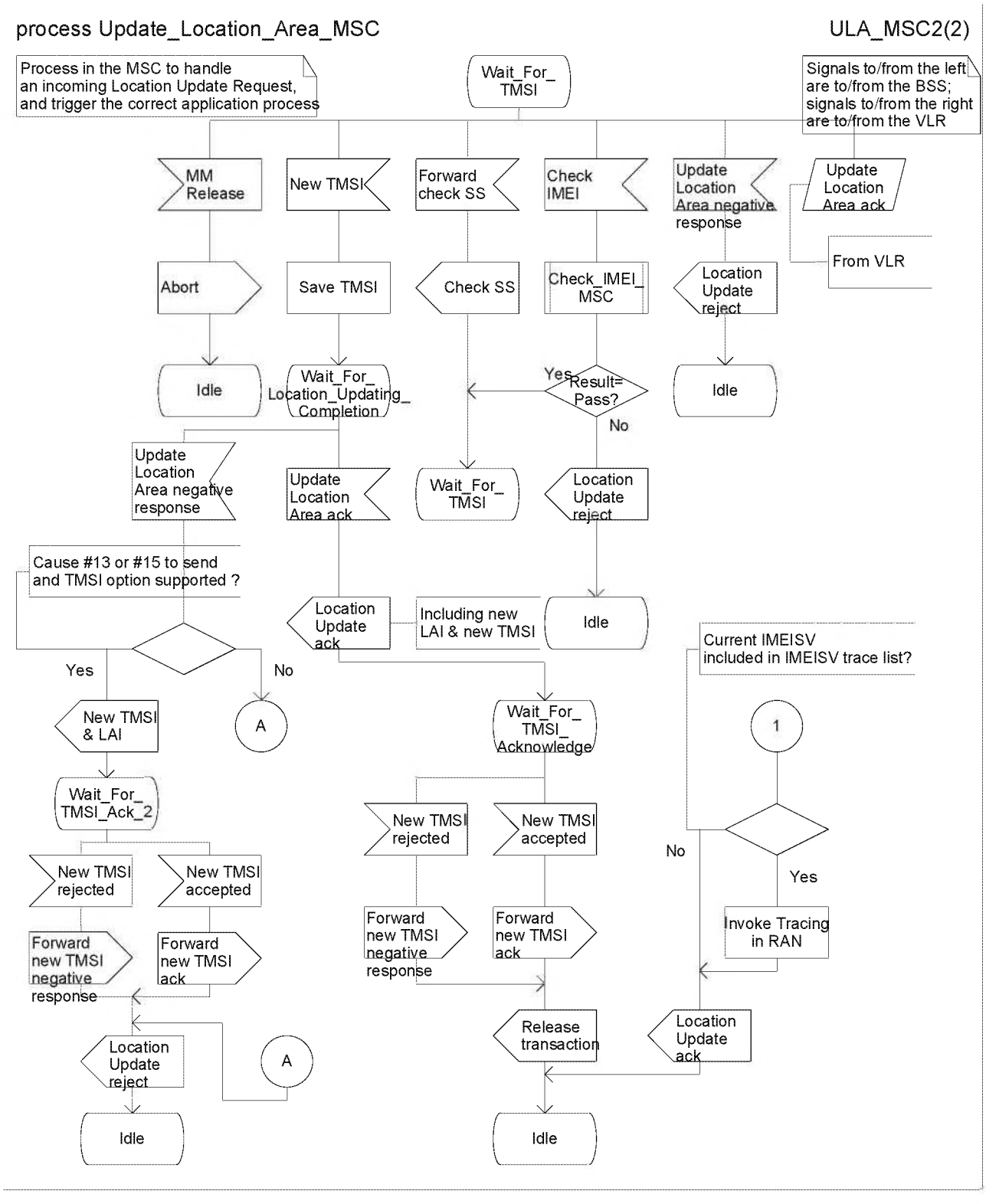

Figure 4.1.1.1 (sheet 2 of 2): Process Update_Location_Area_MSC

4.1.1.2 Procedure Authenticate_MSC

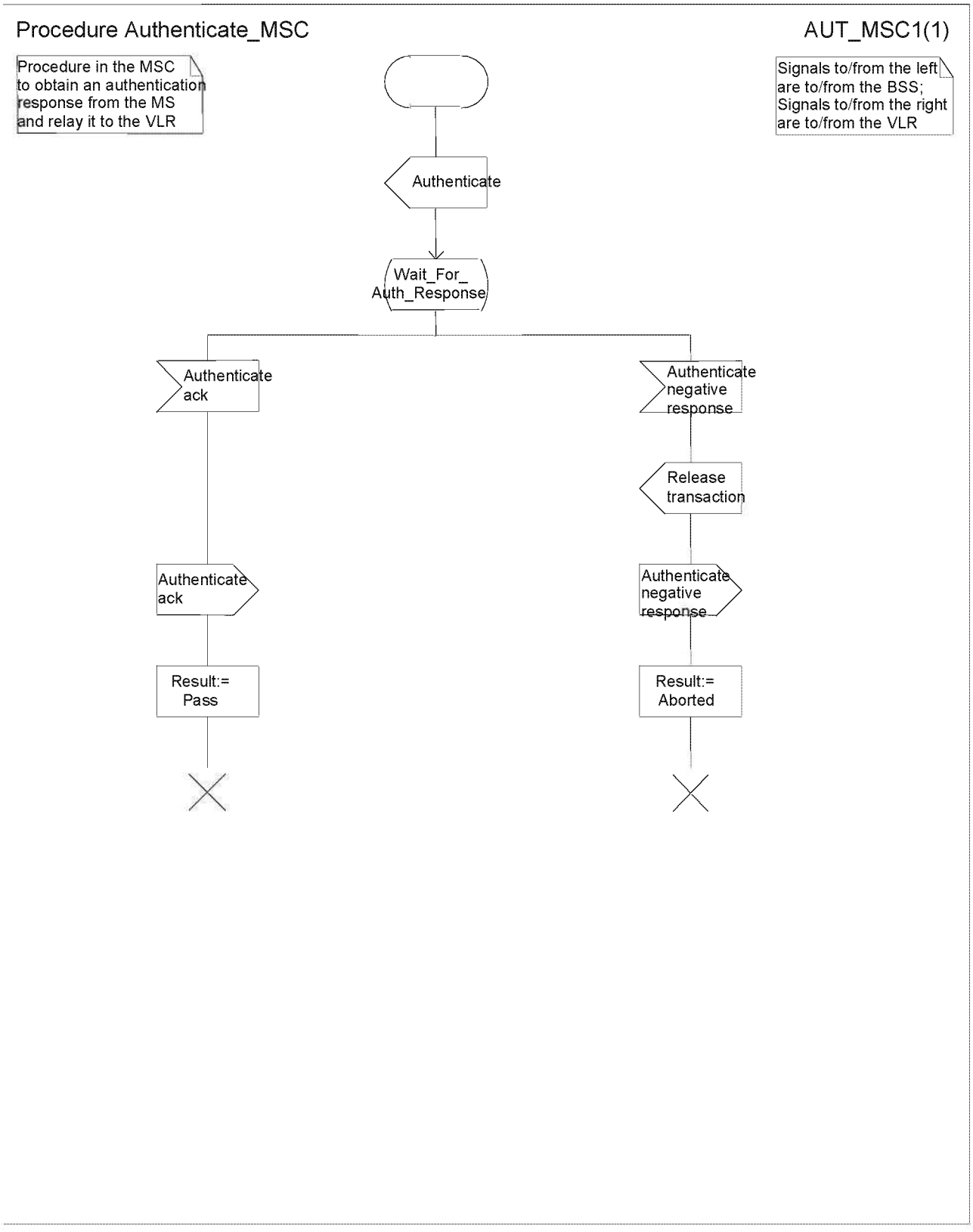

Figure 4.1.1.2 (sheet 1 of 1): Procedure Authenticate_MSC

4.1.2 Detailed procedure in the VLR

4.1.2.1 Process Update_Location_Area_VLR

General comment: at any stage in the location updating process the MSC may receive an indication from the BSS that the MM transaction has been released. The MSC then sends an Abort signal to the VLR. Upon receipt of this message, the VLR shall follow one of two possible courses of action.

The two possible courses of action and the conditions determining which course shall be taken are as follows:

1. If a successfully authenticated radio connection is already established before the Abort message is received, the VLR shall ignore the message.

2. If a successfully authenticated radio connection has not been established before the Abort message is received, the VLR shall abort the Update Location Area process and return to the idle state.

Sheet 1: the location area updating process will be activated by receiving an Update Location Area indication from the MSC. If there are parameter errors in the indication, the process is terminated with the appropriate error sent in the Update Location Area response to the MSC. Else, the behaviour will depend on the subscriber identity received, either an IMSI or a TMSI.

The Automatic Device Detection (ADD) function is an optional feature that allows the HLR to be updated with the current User Equipment (IMEISV) and thus enables the network to configure the subscriber's equipment based on a predefined profile. The mechanism for the IMEISV retrieval by device management system (either from HLR or VLR) is outside the scope of this specification. As an optimisation, the VLR may optionally store whether or not the HLR supports the ADD feature and use this information to decide whether or not to send an update to the HLR.

The Paging Area function is an optional feature that allows the HLR to be updated with the current Paging Area (PgA) (see subclause 2.6). If supported, whenever the paging area changes, the VLR shall send a MAP Update Location request with the Paging Area parameter set to the location areas belonging to the new paging area. The Paging Area is then sent by the HLR (if available) to the VLR in the MAP Provide Roaming Number and may be used for paging optimisation after a MSC/VLR restart (see 3GPP TS 23.018 [5a]).

Sheet 1: The usage of a Hop Counter is an optional optimization.

Sheet 2: at the decision "HLR updating required?" the "True" branch shall be taken if and only if one or more of the following conditions is true:

(1) Location Info Confirmed in HLR is false.

(2) Data Confirmed by HLR is false.

Sheet 2: : The execution of the test "HLR supports ADD?" and the action "set: skip subscriber data update" is an optional optimisation and depends on the presence of the relevant indication from the HLR that ADD functionality is supported. If this optimisation is not supported on the VLR or no indication is received, both are bypassed in which case processing continues at connector 4.

Sheet 2: The execution of the test "HLR supports PgA?" and the action "set: skip subscriber data update" depends on the presence of the relevant indication from the HLR that PgA functionality is supported.

Sheet 2: The "Subscriber data dormant" flag is an optional parameter that shall at least be supported by VLR implementing the Mobile Terminating Roaming Retry feature (see 3GPP TS 23.018 [5a]). A VLR not supporting this flag shall behave as if the flag is set to false.

Sheet 2: A VLR supporting the Mobile Terminating Roaming Retry feature sets the "Cancel Location received" flag to false after authenticating the radio connection. This is used to determine whether to trigger MT roaming retry upon receipt of an incoming call, see subclause 7.3.2.1 of 3GPP TS 23.018 [5a].

Sheet 3: the procedure Obtain_IMSI_VLR is specified in 3GPP TS 23.018 [5a].

The type of Location Update is retrieved in 3GPP TS 23.078 [11] procedure 'Set_Notification_Type' and is returned into the 'Notify' variable; this information is necessary for the CAMEL Mobility Management event notification procedure 3GPP TS 23.078 [11] 'Notify_gsmSCF'.

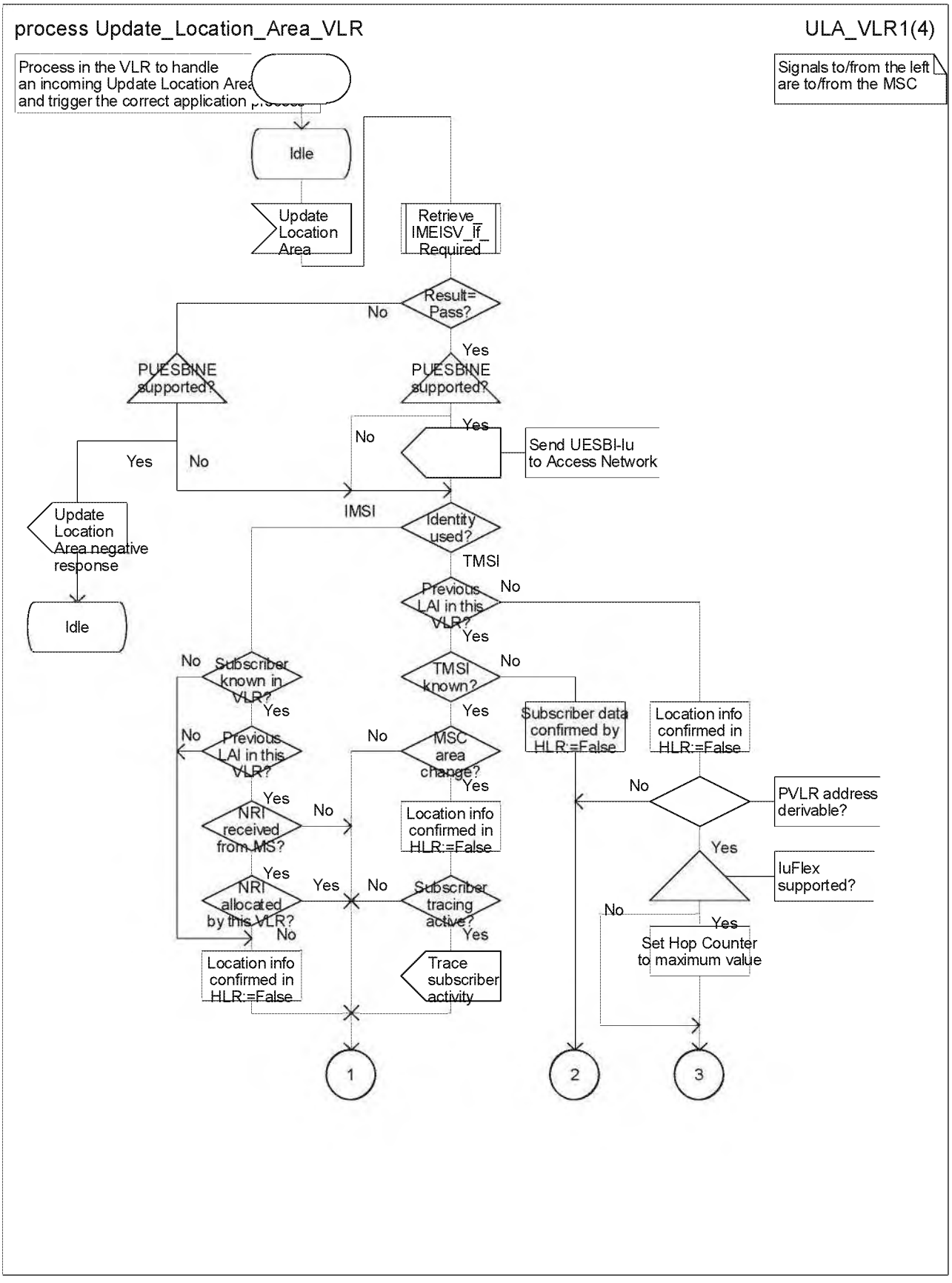

Figure 4.1.2.1 (sheet 1 of 3): Process Update_Location_Area_VLR

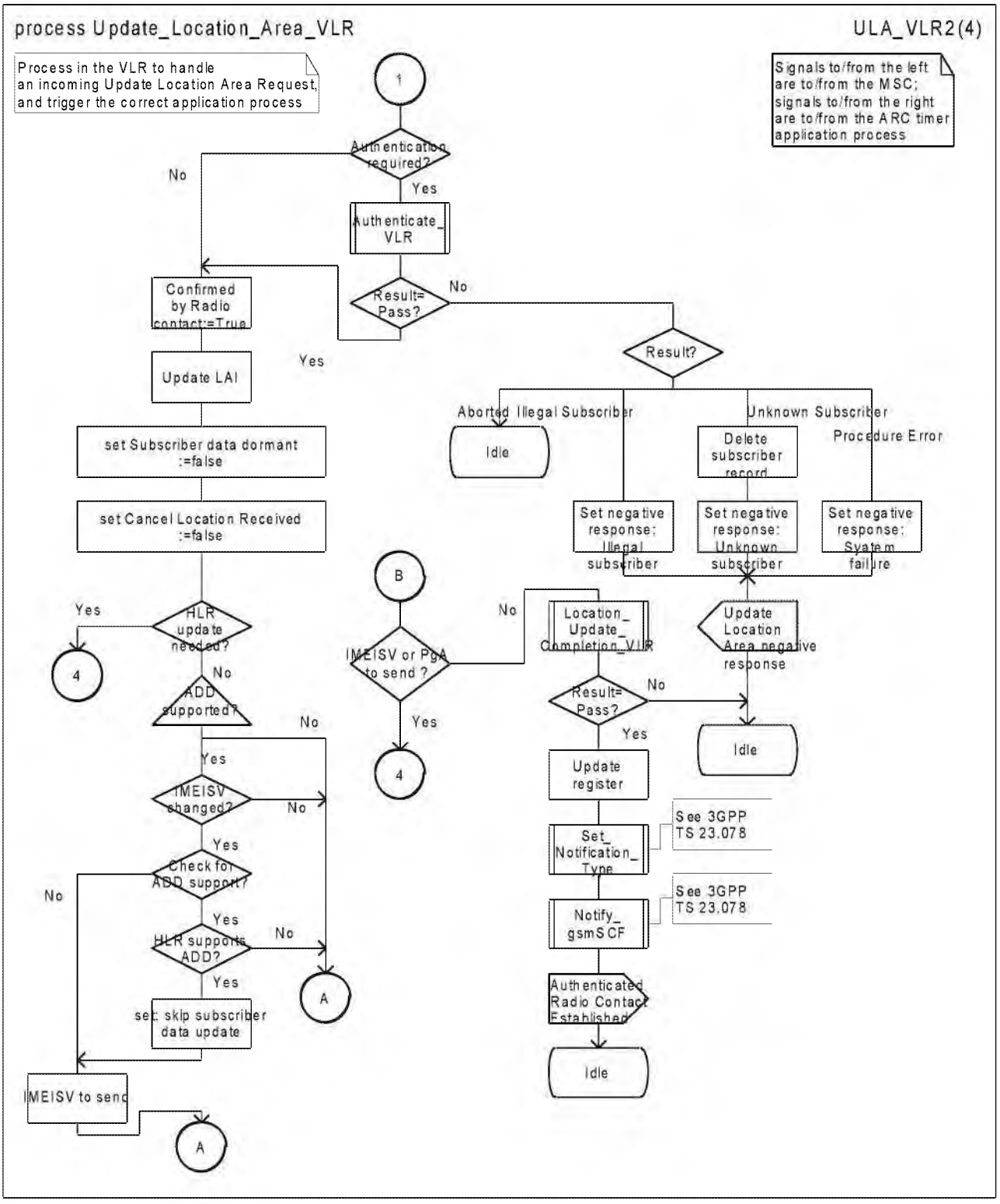

Figure 4.1.2.1 (sheet 2 of 3): Process Update_Location_Area_VLR

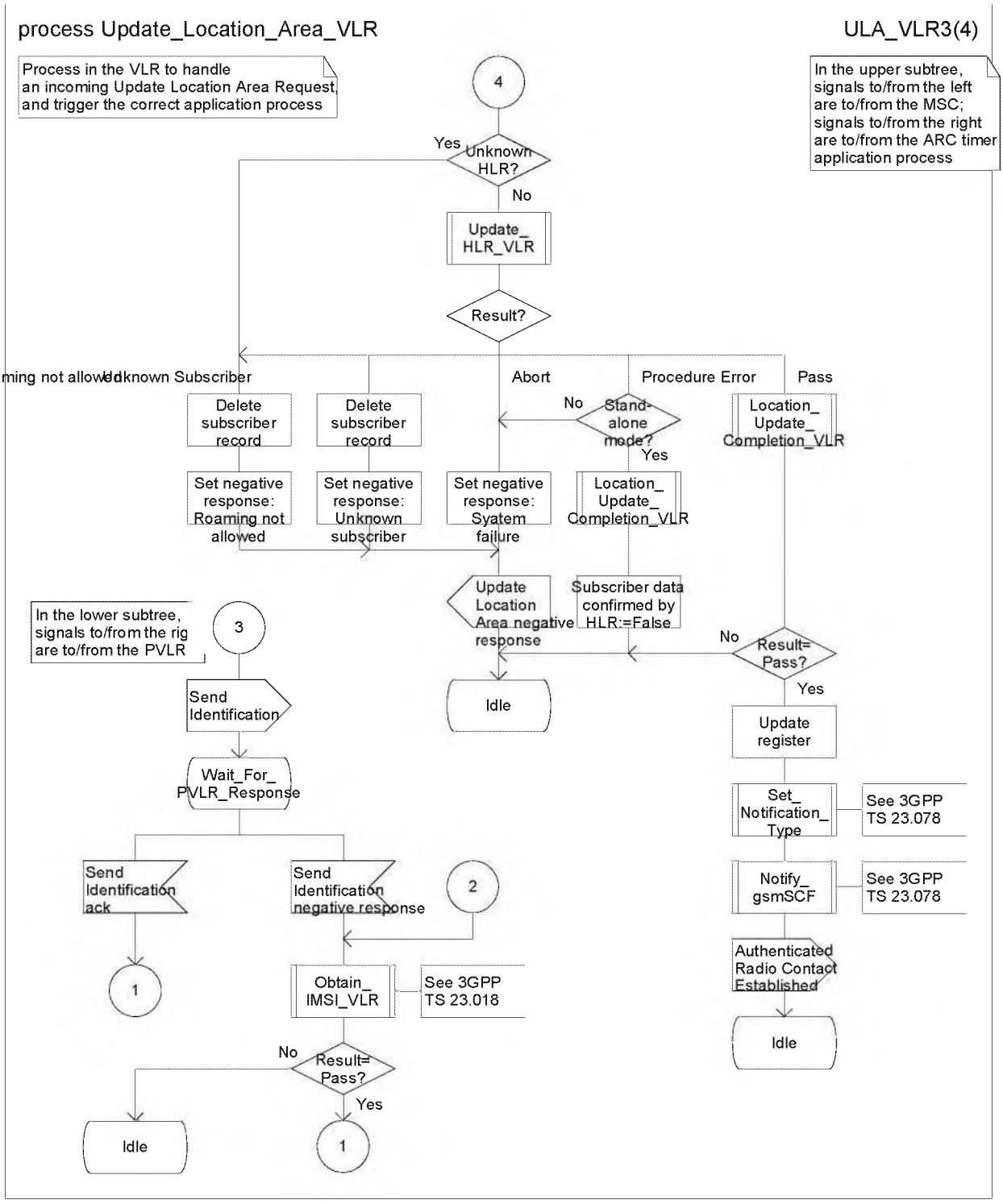

Figure 4.1.2.1 (sheet 3 of 3): Process Update_Location_Area_VLR

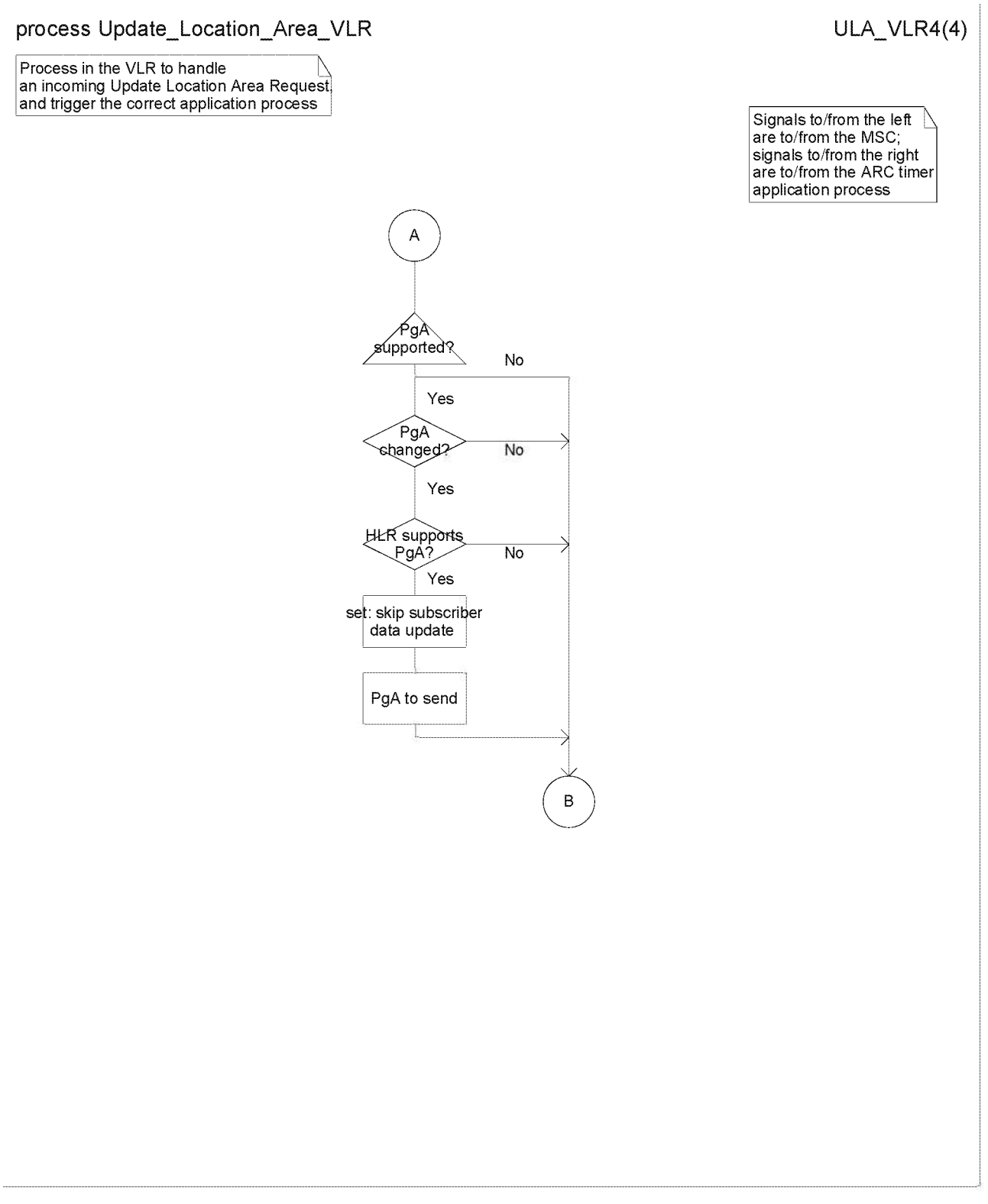

Figure 4.1.2.1 (sheet 4 of 4): Process Update_Location_Area_VLR

4.1.2.1a Procedure Retrieve_IMEISV_If_Required

The decision box "received IMEISV = stored IMEISV" takes the "No" exit if no IMEISV is stored.

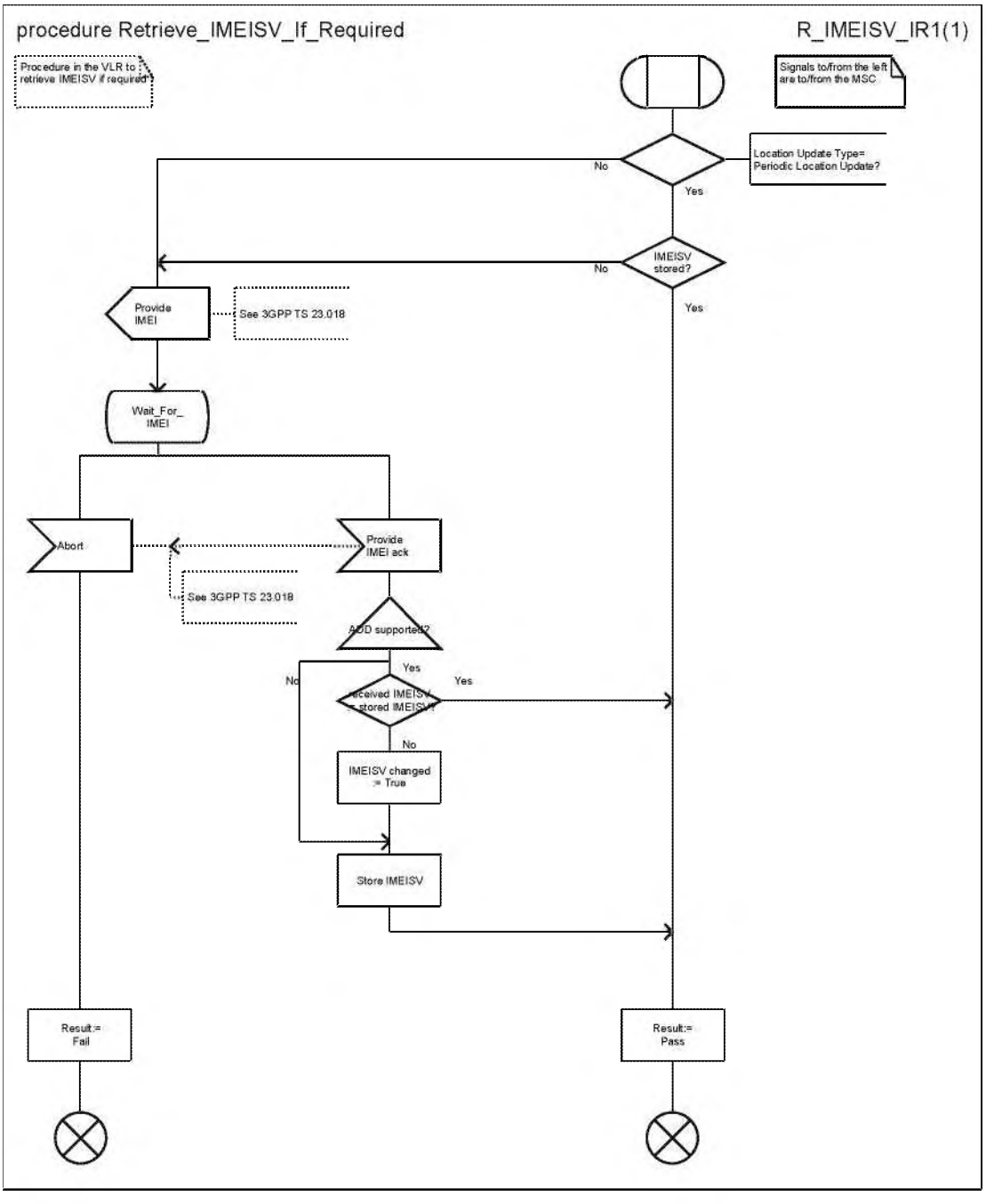

Figure 4.1.2.1A: Procedure Retrieve_IMEISV_If_Required

4.1.2.2 Procedure Authenticate_VLR

Sheet 2: The procedure Obtain_IMSI_VLR is specified in 3GPP TS 23.018 [5a].

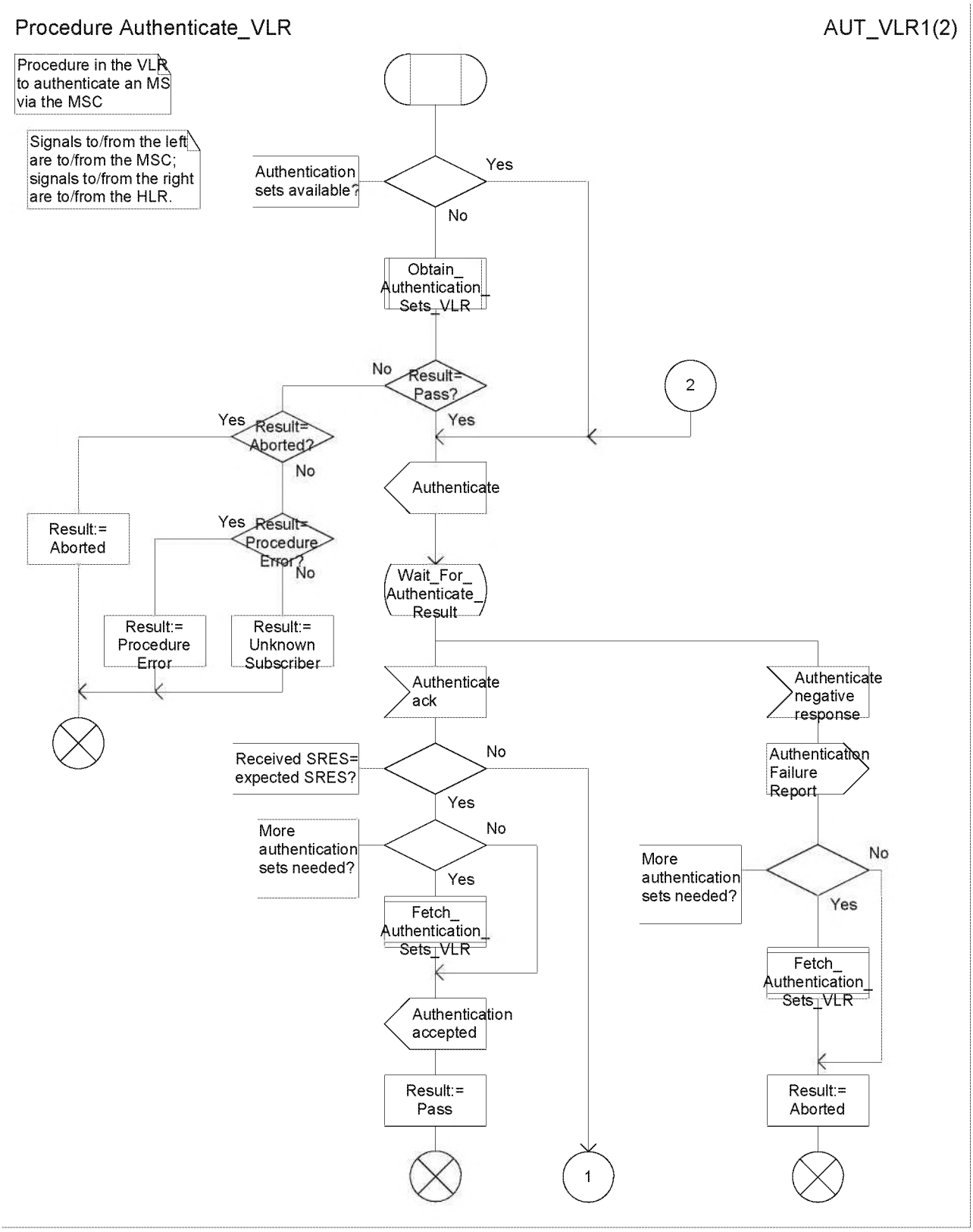

Figure 4.1.2.2 (sheet 1 of 2): Procedure Authenticate_VLR

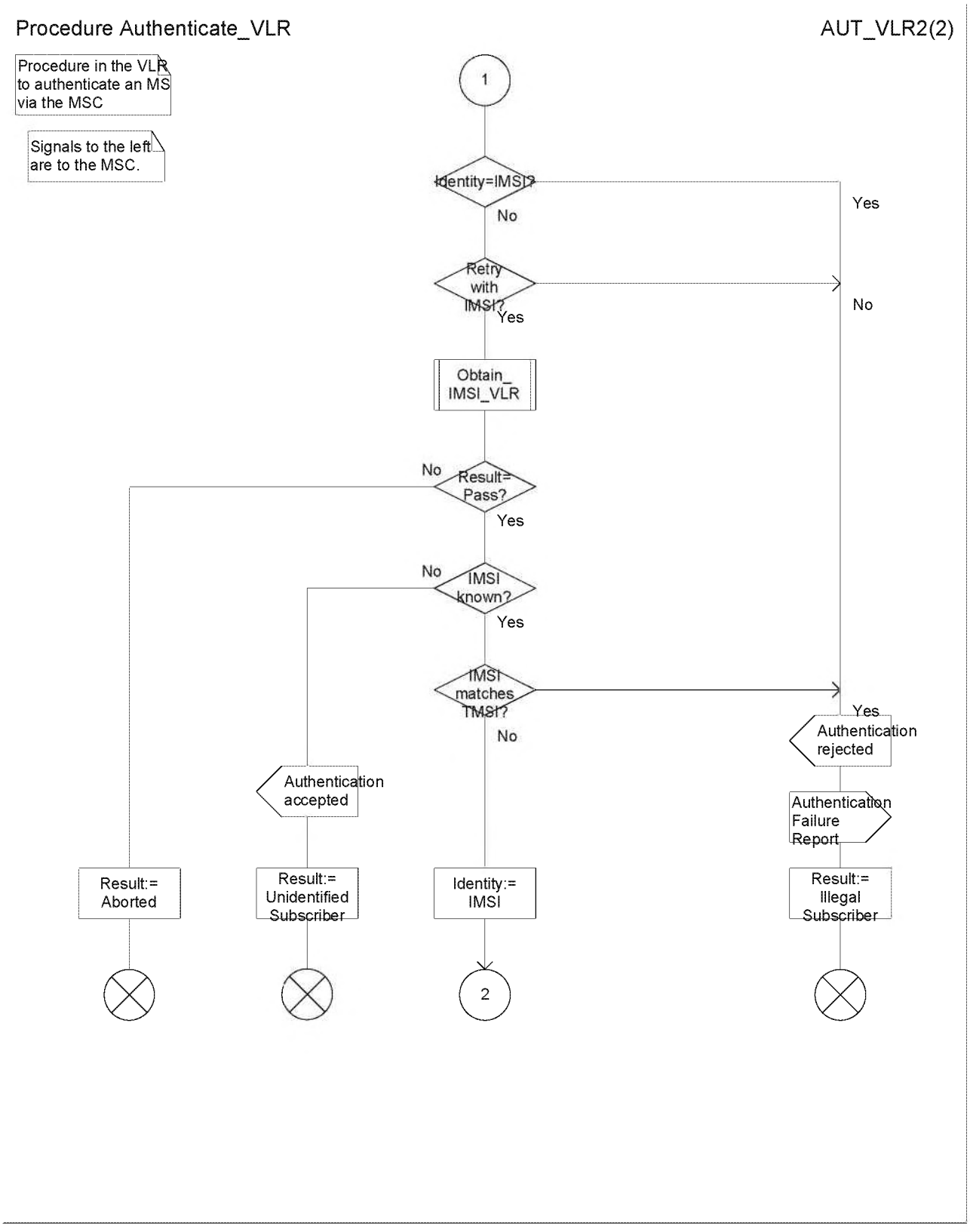

Figure 4.1.2.2 (sheet 2 of 2): Procedure Authenticate_VLR

4.1.2.3 Procedure Location_Update_Completion_VLR

Sheet 1: Decision "National Roaming Restrictions Exist?" distinguishes whether or not the subscriber is allowed service in the target LA, based on the current location of the MS and the VLR's knowledge of other networks. The "Yes" branch results in the sending of "Update Location Area Negative Response" toward the MSC (and the MS), with cause "National Roaming Not Allowed." However, subscriber data shall not be deleted from the VLR. This is to avoid unnecessary HLR updating should the subscriber be allowed subsequently to roam in other LAs of the same MSC.

Sheet 1: Decision "Access-Restriction-Data permits current RAT?" performs a check on the subscriber's AccessRestrictionData information received from the HLR and either allows the operation to continue or rejects the Location Update. The decision is taken according to the following:

-If AccessRestrictionData value includes "GERAN not allowed" and the LA/RA, where the MS accesses the network, is served by GERAN, then the subscriber's access is not permitted.

-If AccessRestrictionData value includes "UTRAN not allowed" and the LA/RA, where the MS accesses the network is served by UTRAN, then the subscriber's access is not permitted.

Sheet 1: When the Location Update is not allowed because the subscriber access is restricted due to Administrative Restriction of Subscribers' Access feature, the flow results in the sending of "Update Location Area Negative Response" toward the MSC (and the MS). The recommended cause code is "RAT not allowed", but cause codes "PLMN not allowed" or "National Roaming Not allowed" may also be used based on operator configuration and the required MS behaviour.

Note: For the mapping of MAP Process cause code values to values on the MM protocol interface see 3GPP TS 29.010 [14].
For the MS behaviour determined on the received cause code see 3GPP TS 24.008[13].

Sheet 1: Decision "Roaming restriction due to Unsupported Feature received in subscriber data?" distinguishes whether or not the subscriber data received from the HLR indicates "roaming restriction due to unsupported feature." The "Yes" branch results in the sending of "Update Location Area Negative Response" toward the MSC (and the MS), with cause "National Roaming Not Allowed." However, subscriber data shall not be deleted from the VLR. This is to avoid unnecessary HLR updating should the subscriber be allowed subsequently to roam in other LAs of the same MSC.

Sheet 1: Decision "Regional subscription restriction" distinguishes whether or not the subscriber is allowed service in the target LA, which the VLR deduces based on regional subscription information received from the HLR. The "Yes" branch results in the sending of "Update Location Area Negative Response" toward the MSC (and the MS), with cause "location area not allowed." However, subscriber data shall not be deleted from the VLR. This is to avoid unnecessary HLR updating should the subscriber be allowed subsequently to roam in other LAs of the same MSC.

Sheet 1: Causes "National Roaming Not Allowed" and "RAT not allowed" lead to sending of cause #13 (roaming not allowed in the Location Area) and #15 (no suitable cells in Location Area) respectively to the MS (see 3GPP TS 29.010 [14]). On receipt of cause #13 or #15 the TMSI and LAI currently stored in the MS are not deleted (see 3GPP TS 24.008 [13]). As an option (referred-to as "TMSI option"), for these two reject causes, the VLR may forward a new TMSI (with the new LAI) together with the sending of "Update Location Area Negative Response" toward the MSC. The Location Updating Reject is sent to the MS after forwarding of the new TMSI (and new LAI) (see subclause 4.1.1.1).

This optional TMSI allocation (with new LAI) ensures that:

- a pre-Rel-8 MS will initiate a location updating if it roams back to the previous Location Area (allowed), i.e. to the location area whose identity is already stored in the MS, after having received the reject cause #13 or #15; otherwise the location updating may not be initiated and mobile terminated calls may not be delivered until the next mobile originated activity or periodic location update (see 3GPP TR 29.994 [18]).

- the next location update enables the new VLR to address the correct previous VLR (which controls the not allowed Location Area) and to obtain the right IMSI and security context; otherwise a wrong VLR is addressed (corresponding to the TMSI/LAI of the VLR that controlled the previous allowed LA) and a wrong IMSI / security context would be obtained if the TMSI was reallocated.

Sheet 2: If the MS performs a location update procedure in a VPLMN supporting Autonomous CSG Roaming and the HPLMN has enabled Autonomous CSG Roaming in the VPLMN (via Service Level Agreement) and if the VLR needs to retrieve the CSG Subscription Data of the MS from the CSS, the VLR shall initiate the Update VCSG Location

Procedure with the CSS and store the CSG Subscription data if any received from the CSS. The stored CSG Subscription data is used by VLR to perform access control for the MS.

If the Update VCSG Location Procedure fails, the VLR continues the location update procedure.

Sheet 3: The procedure Check_IMEI_VLR is specified in 3GPP TS 23.018 [5a].

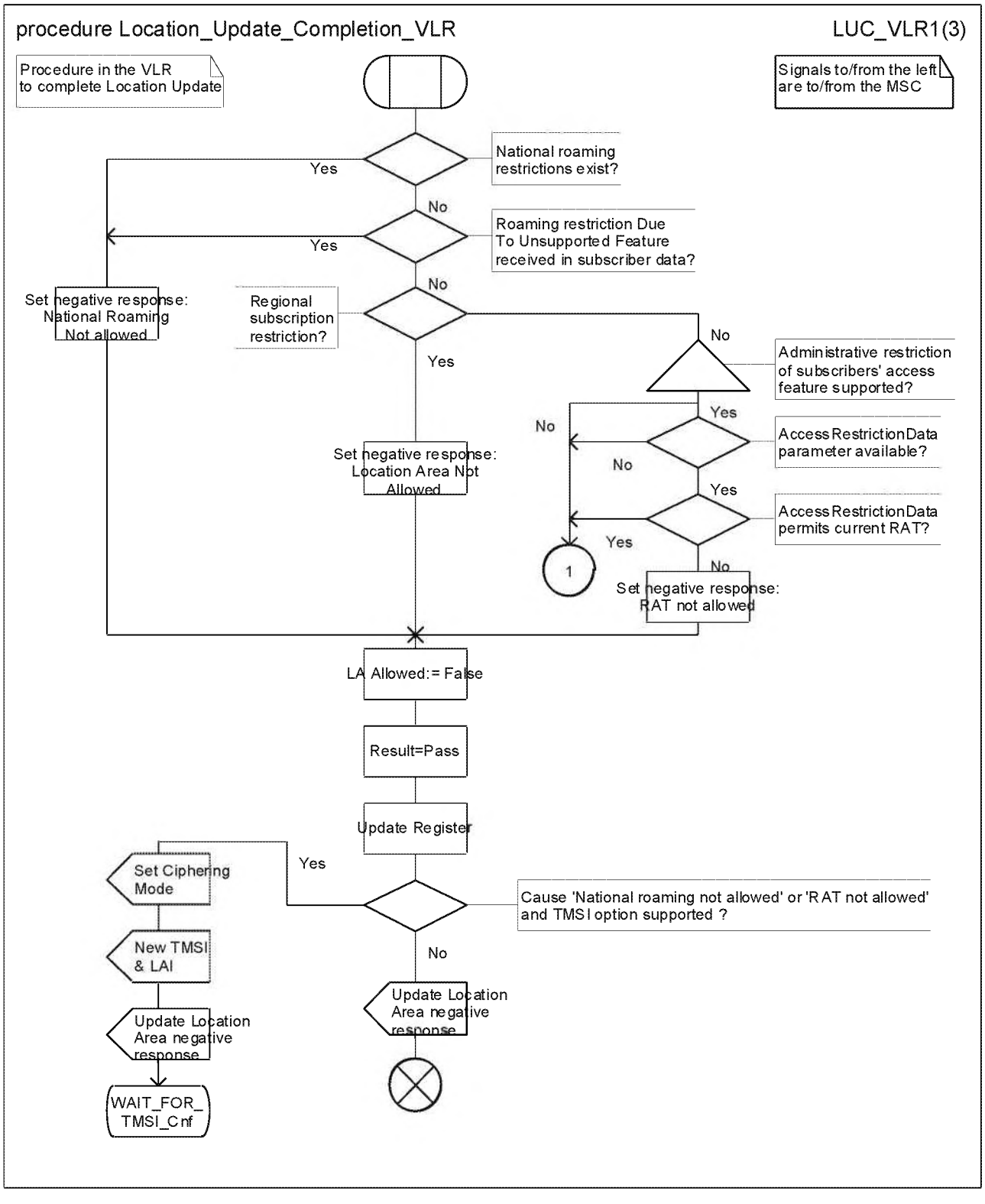

Figure 4.1.2.3 (sheet 1 of 3): Procedure Location_Update_Completion_VLR

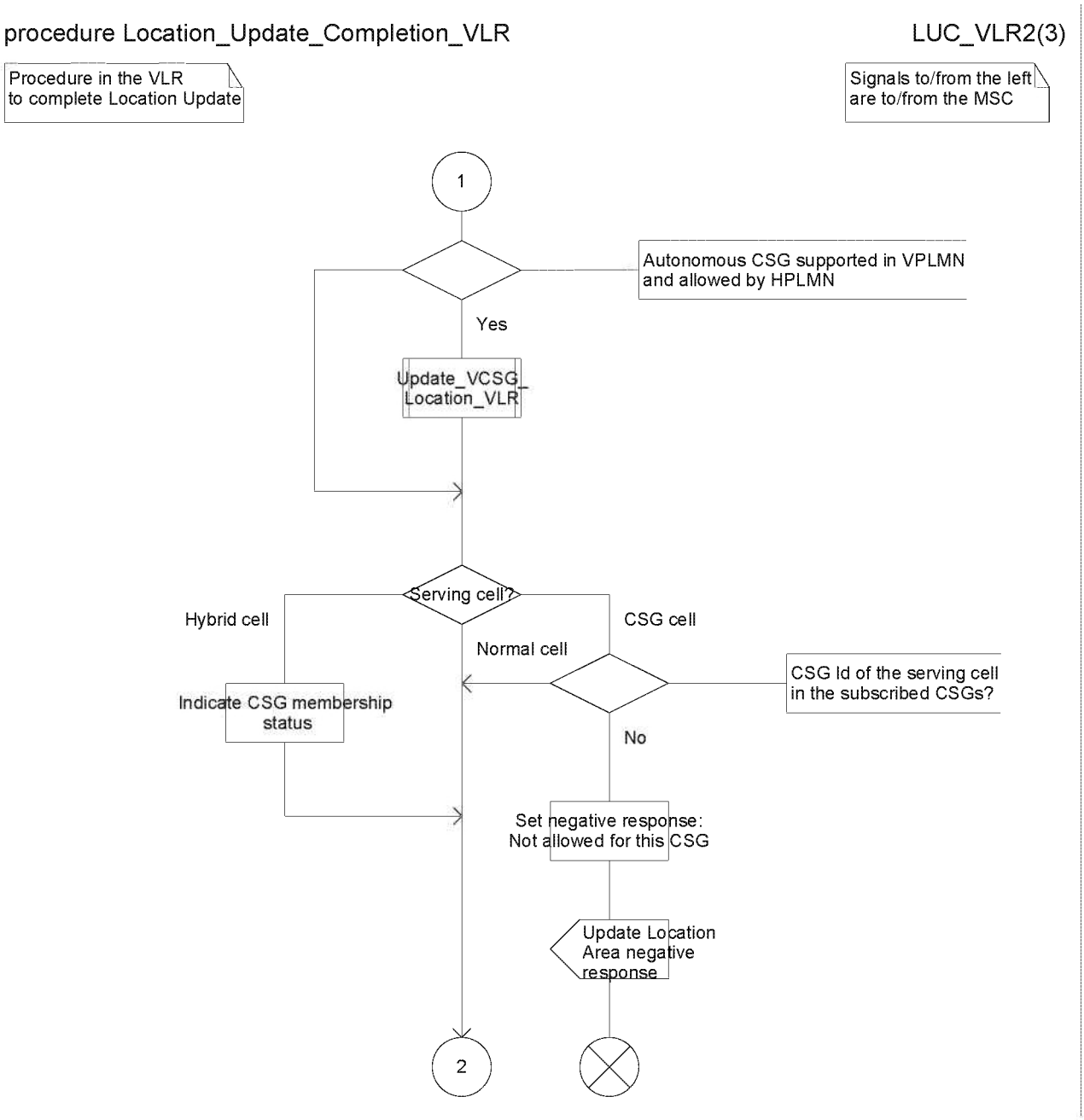

Figure 4.1.2.3 (sheet 2 of 3): Procedure Location_Update_Completion_VLR

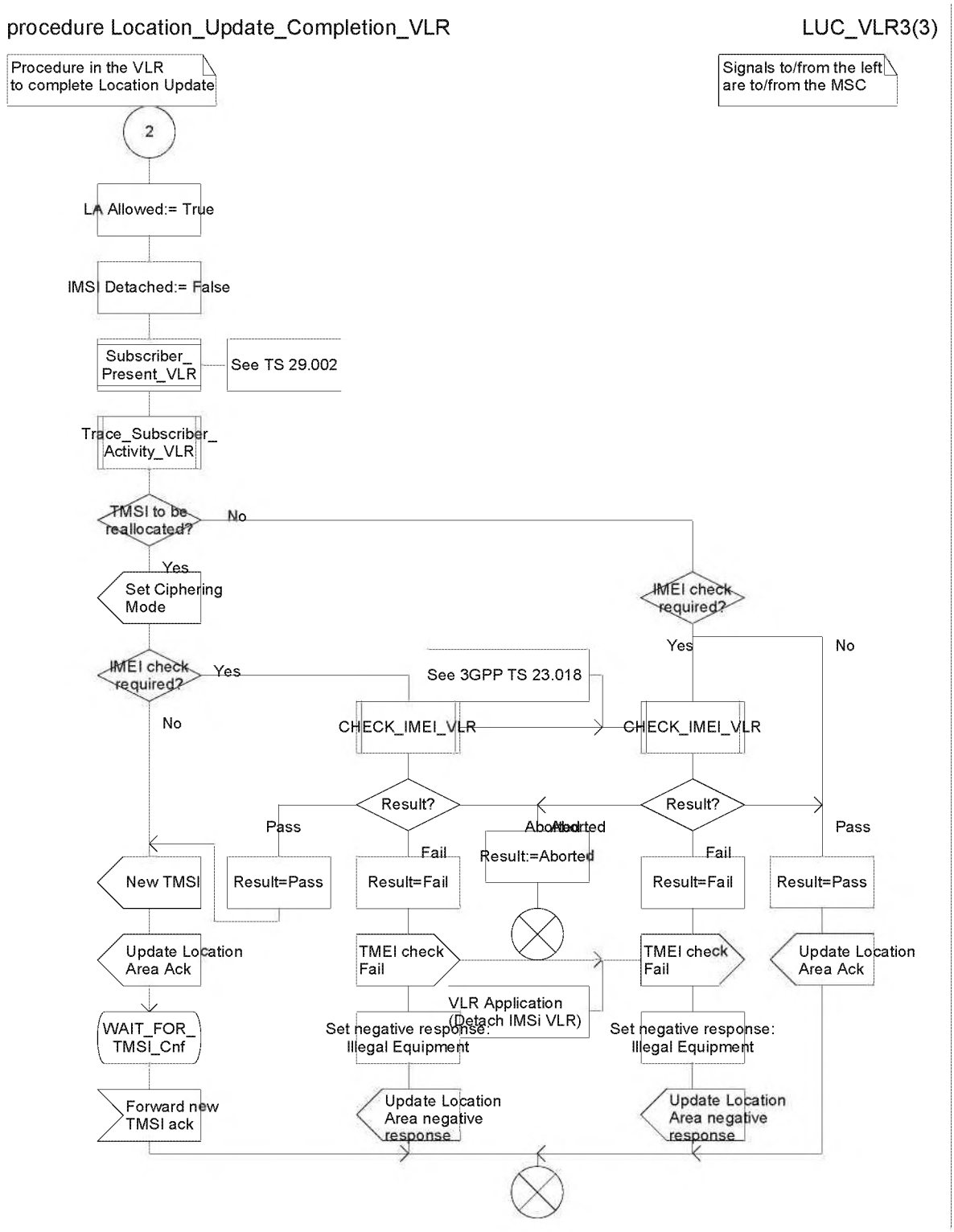

Figure 4.1.2.3 (sheet 3 of 3): Procedure Location_Update_Completion_VLR

4.1.2.4 Procedure Update_HLR_VLR

Sheet 1: The procedure Check_User_Error_In_Serving_Network_Entity is specific to Super-Charger; it is specified in 3GPP TS 23.116 [7].

Sheet 1: A VLR supporting the MT Roaming Forwarding feature (see 3GPP TS 23.018 [5a]) includes the "MTRF supported" flag in the MAP Update Location message sent to the HLR. After sending this message, the VLR may receive at any time an MT Provide Roaming Number request including the MTRF Indicator from the old VLR in the WAIT_FOR_DATA state *(not represented in the SDL)*.

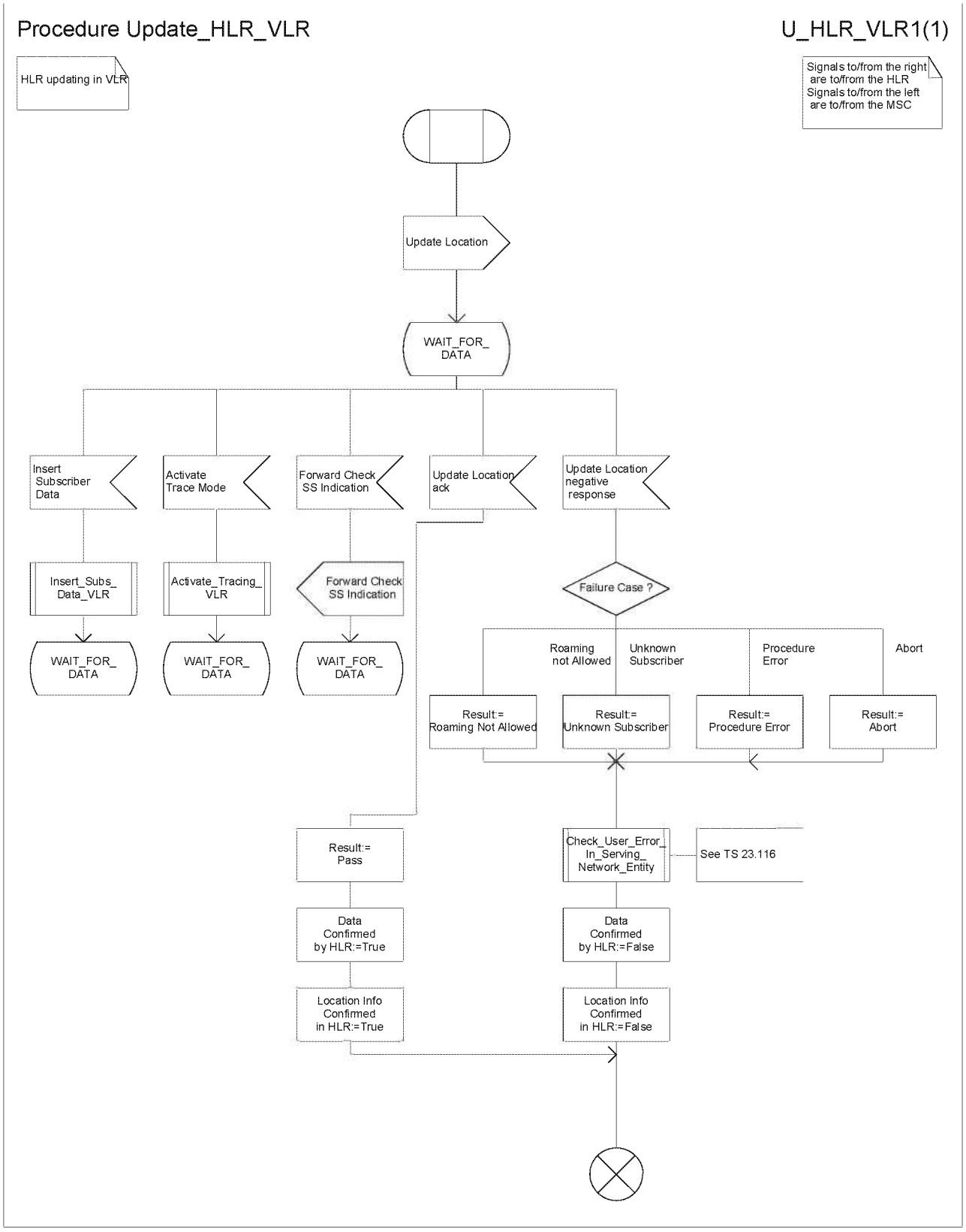

Figure 4.1.2.4 (sheet 1 of 1): Procedure Update_HLR_VLR

4.1.2.5 Procedure Insert_Subs_Data_VLR

The procedure Check_Parameters is specified in 3GPP TS 23.018 [5a].

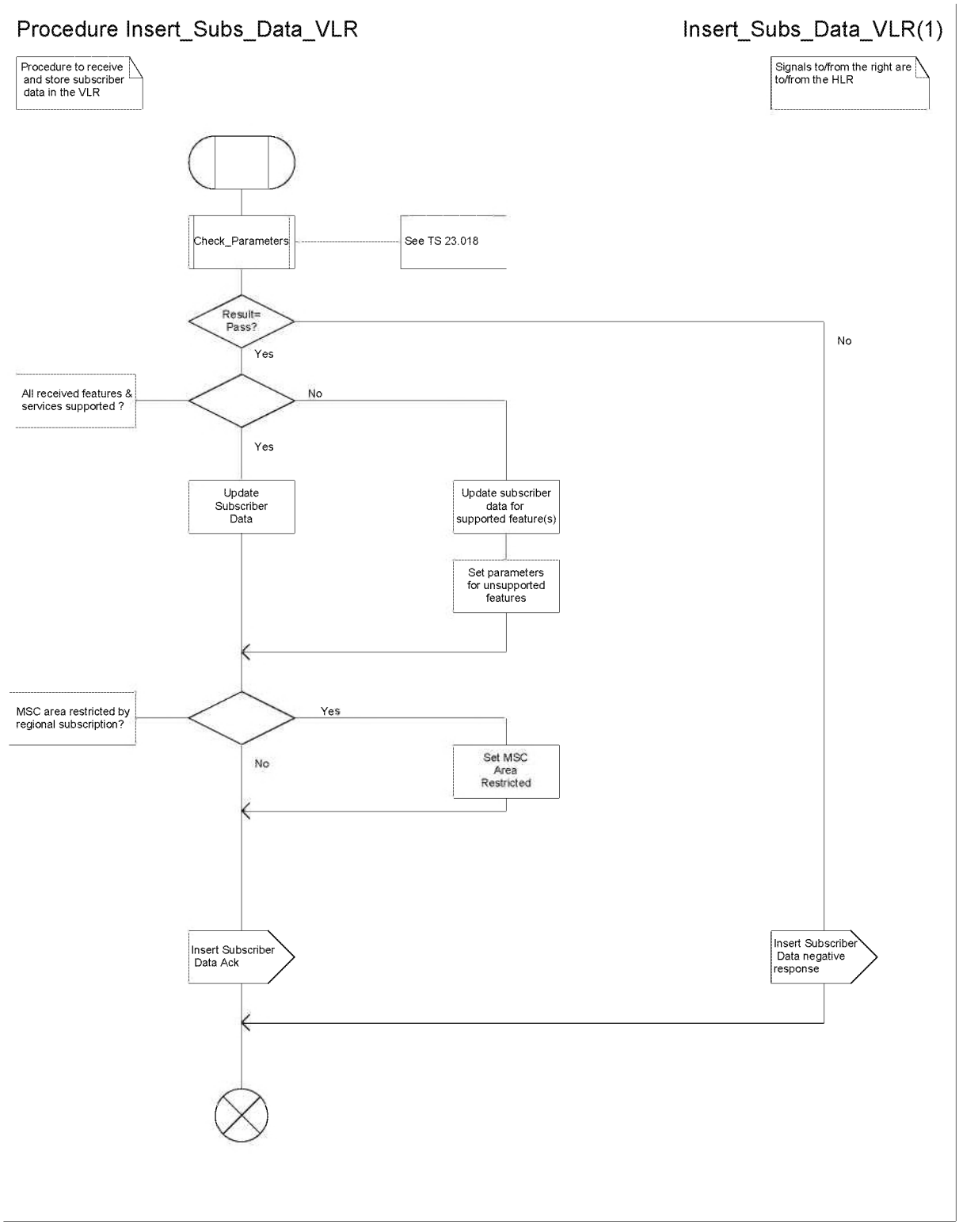

Figure 4.1.2.5 (sheet 1 of 1): Procedure Insert_Subs_Data_VLR

4.1.2.6 Procedure Activate_Tracing_VLR

The procedure Check_Parameters is specified in 3GPP TS 23.018 [5a].

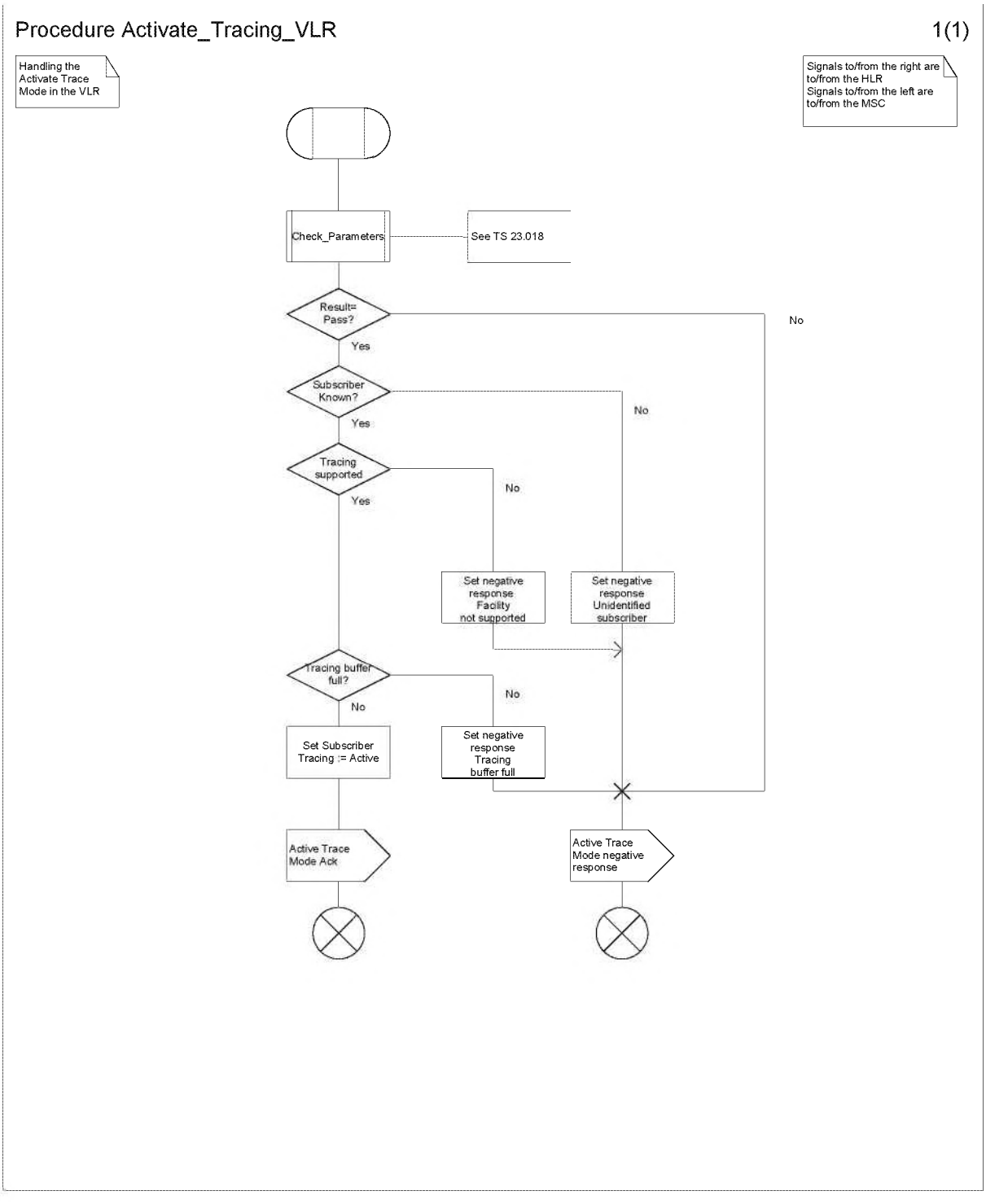

Figure 4.1.2.6 (sheet 1 of 1): Procedure Activate_Tracing_VLR

4.1.2.7 Process Send_Identification_PVLR

Sheet 1: The procedure Check_Parameters is specified in 3GPP TS 23.018 [5a].

Sheet 1: Decision "IuFlex applied?" distinguishes whether or not the PVLR applies "Intra Domain Connection of RAN Nodes to Multiple CN Nodes" as described in 3GPP TS 23.236 [12]. If this feature is applied, the VLR shall extract the NRI from the TMSI and attempt to derive the VLR address of the VLR where the subscriber was previously registered, denoted in the following as the "real PVLR".

Sheet 1: Decision "Result = success?" distinguishes whether the NRI could be successfully converted into the "real PVLR" address. In case of successful conversion, the PVLR shall relay the received Send_Identification message to the "real PVLR" as specified in 3GPP TS 23.236 [12]. The new VLR and the "real PVLR" shall not perceive that relaying is being performed, i.e. they shall not notice the presence of the relaying node. The actual mechanism used to perform the relay is an implementation choice. A possible mechanism is described in section 4.1.2.9.

Sheet 1: If supported by the VLR, the "Subscriber data dormant" flag shall be set to true to reflect that the MS has moved outside the VLR area. A VLR not supporting this flag shall behave as if the flag is set to false.

NOTE: HLRs compliant with this release of the specification and supporting mobile terminating roaming retry and Super-Charger will always send a Cancel Location message to the old VLR even in a supercharged network (see 3GPP TS 23.018 [5a]). HLRs compliant with an earlier release of the specification may not always send a Cancel Location message in a supercharged network. To support mobile terminating roaming retry with such HLR implementations, the old VLR can start a timer upon receipt of the MAP Send Identification message while on-going paging to trigger the sending of an internal Cancel Location to the old MSC and thus the sending of a MAP Resume Call Handling message by the old MSC to the GMSC after the sending of the MAP Update Location by the new VLR to the HLR.

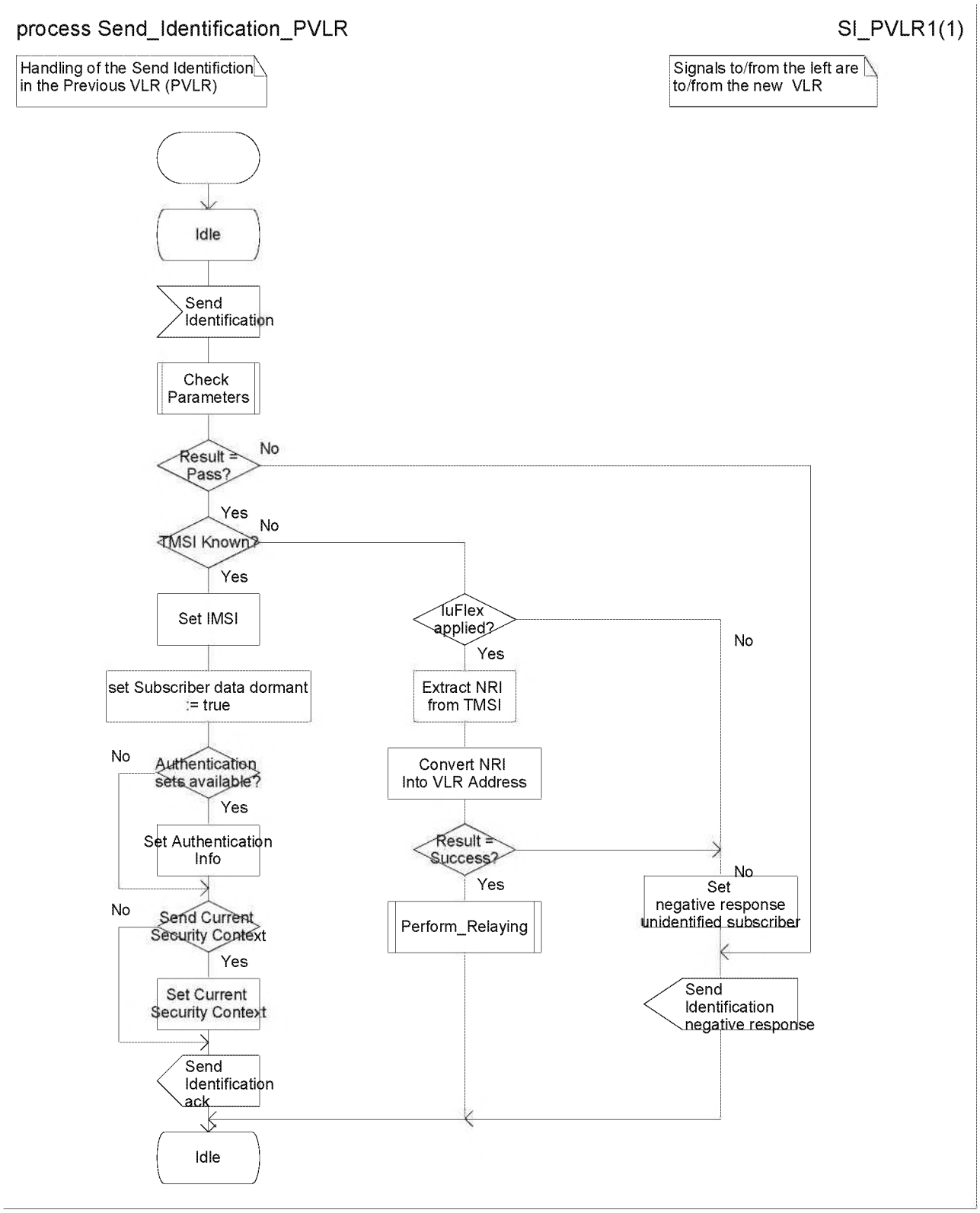

Figure 4.1.2.7 (sheet 1 of 1): Process Send_Identification_PVLR

4.1.2.8 Process Trace_Subscriber_Activity_VLR

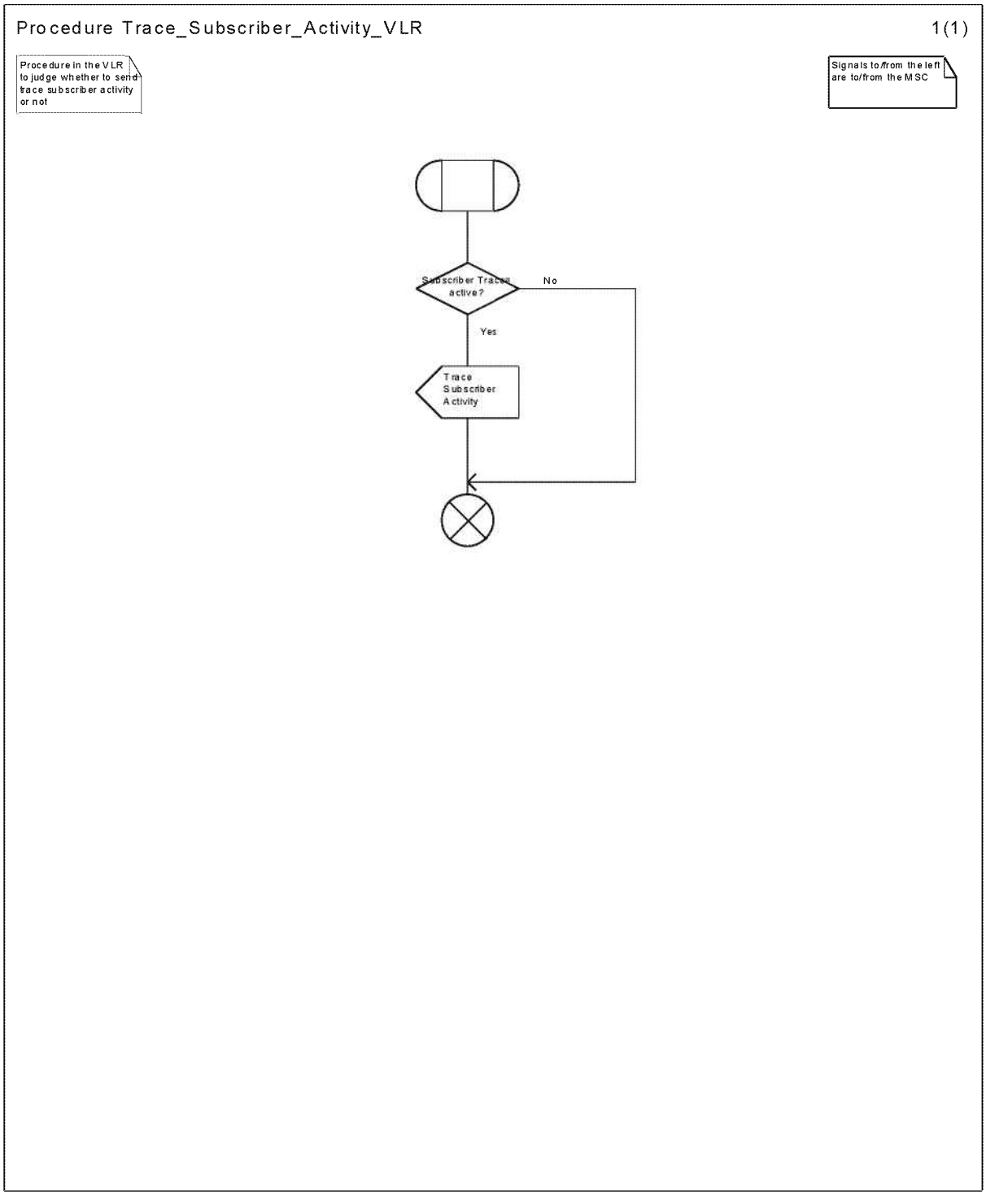

Figure 4.1.2.8 (sheet 1 of 1): Process Trace_Subscriber_Activity_VLR

4.1.2.9 Procedure Perform Relaying

The relay may be performed by opening a new MAP dialogue to the "real PVLR" and keeping it linked to the existing MAP dialogue between the new VLR and the PVLR. Every message received for one of these dialogues shall be relayed to the other one, until the two dialogues are closed. This mechanism is described in figure 4.1.2.9.

In order to improve the signalling efficiency of the relaying function, alternative mechanisms may be implemented as long as no difference shall be perceived by the new VLR and the "real PVLR".

The usage of a Hop Counter is an optional optimization.

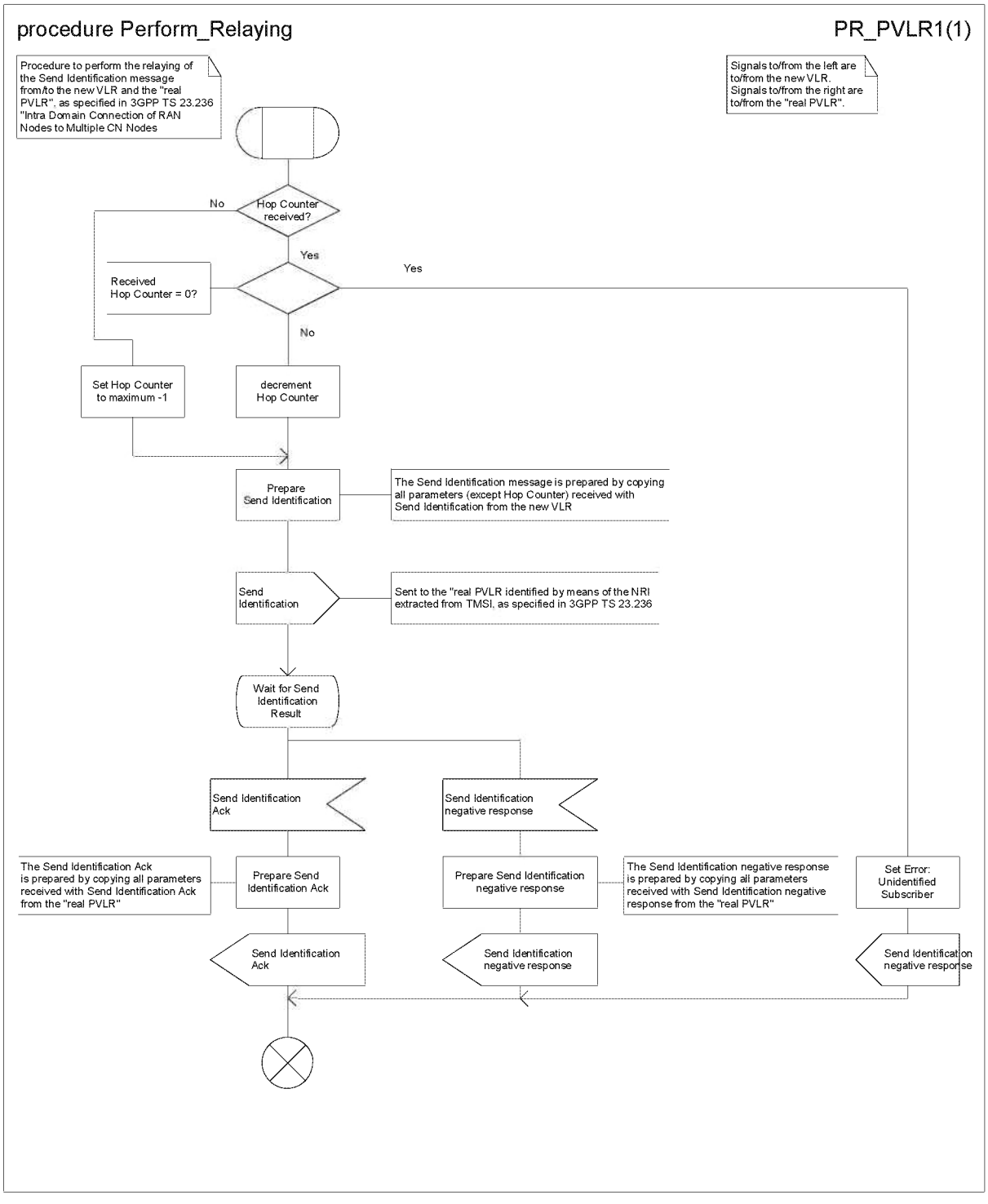

Figure 4.1.2.9 (sheet 1 of 1): Procedure Perform Relaying

4.1.2.10 Procedure Update_VCSG_Location_VLR

The VLR uses this procedure to register the MS with the CSG Subscriber Server and may retrieve the CSG subscription data from CSS.

When using this procedure, the VLR sends an Update VCSG Location request towards the CSS, and waits for the answer from the CSS.

- If the VLR receives a negative Update VCSG Location response from the CSS, the VLR sets the result with failure cause and ends this procedure.
- If the VLR receives an Insert VCSG Subscriber Data request, it shall update the CSG Subscription Data and returns a response message to CSS. The CSG Subscription Data received from the CSS is stored and managed in the VLR independently from the CSG Subscription Data received from the HLR. If the same CSG ID exists in both CSG Subscription Data from the CSS and CSG Subscription Data from the HLR, the CSG Subscription Data from the HLR shall take precedence over the CSG Subscription Data from the CSS.
- If the VLR receives a successful Update VCSG Location ACK message, it ends the procedure.
  - If the successful Update VCSG Location ACK message indicates that there is no CSG Subscription data, the VLR shall not send any subsequent Update VCSG Location Request message to the CSS.

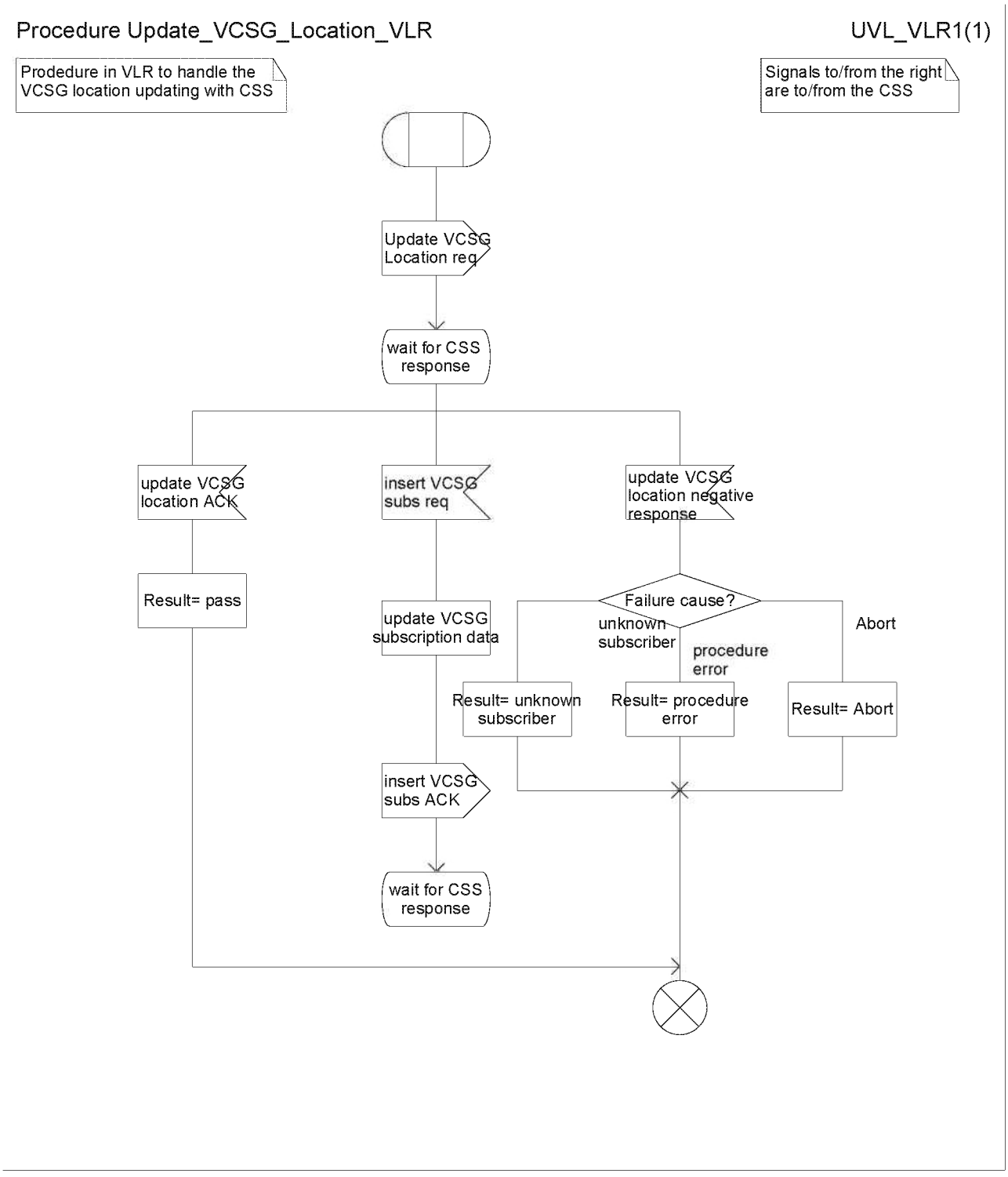

Figure 4.1.2.10 (sheet 1 of 1): Procedure Update_VCSG_Location_VLR

4.1.2.11 Procedure Insert_VCSG_Subs_Data_VLR

Whenever the CSG subscription data is changed for a MS in the CSS, and the changes affect the CSG subscription data stored in the VLR, the CSS shall inform the VLR about the changes by the means of an Insert VCSG Subscriber Data request (IMSI, CSG subscription data) which initiates the procedure Insert_VCSG_Subs_Data_VLR.

The VLR checks the received parameters. If the MS is unknown, the VLR shall send a negative Insert VCSG Subscriber Data response message to the CSS that deregisters the VLR for this MS. If the MS is known, the VLR shall update the stored CSG subscription data and acknowledge the Insert VCSG Subscriber Data request by returning an Insert VCSG Subscriber Data Ack.

The CSG Subscription Data received from the CSS is stored and managed in the VLR independently from the CSG Subscription Data received from the HLR. The Insert VCSG Subscriber Data procedure shall only affect the CSG Subscription Data received from the CSS.

If the same CSG ID exists in both CSG Subscription Data from the CSS and CSG Subscription Data from the HLR, the CSG Subscription Data from the HLR shall take precedence over the CSG Subscription Data from the CSS.

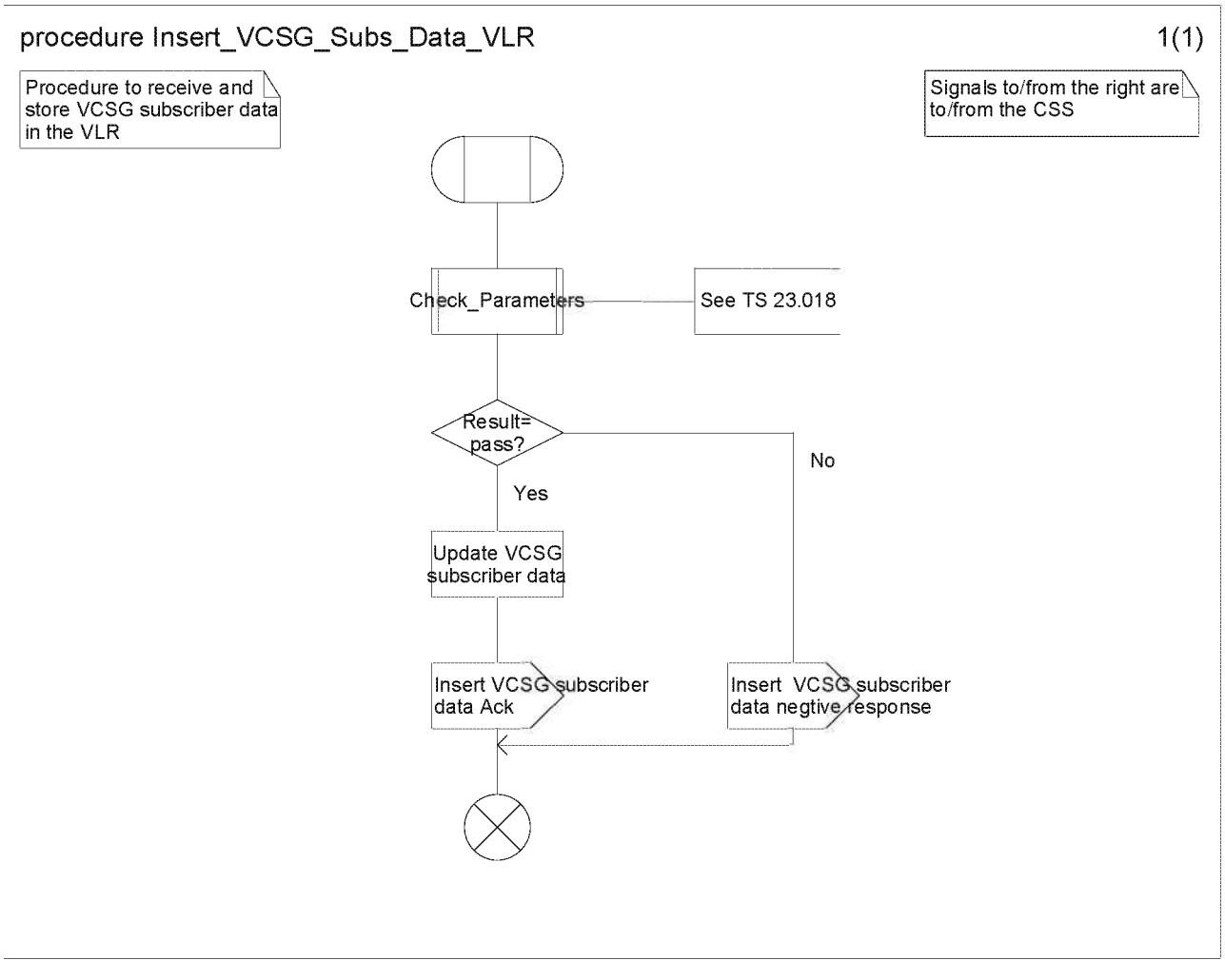

Figure 4.1.2.11 (sheet 1 of 1): Procedure Insert_VCSG_Subs_Data_VLR

4.1.3 Detailed procedure in the HLR

4.1.3.1 Process Update_Location_HLR

The Paging Area function is an optional feature that allows the HLR to be updated with the current Paging Area (PgA) (see subclause 2.6). If supported, the HLR shall store the Paging Area received from the VLR in MAP Update Location requests. If the Paging Area parameter is not included in a MAP Update Location request and the VLR has not changed, the HLR shall keep the stored Paging Area. If the Paging Area parameter is not included in a MAP Update Location request and the VLR has changed, the HLR shall delete the stored Paging Area.

Sheet 1: The procedure Check_Parameters is specified in 3GPP TS 23.018 [5a].

Sheet 1: The procedure Super_Charged_Cancel_Location_HLR is specific to Super-Charger; it is specified in 3GPP TS 23.116 [7]. Sheet 2: The procedure Super_Charged_Location_Updating_HLR is specific to Super-Charger; it is specified in 3GPP TS 23.116 [7]. If subscription data needs to be sent to the VLR, processing continues from the "No" exit of the test "Result=Pass?".

Sheet 2: The execution of the test "skip subscriber data update?" is optional and depends on the presence of the relevant indication from the VLR. If no indication is received, then the result of the test is "No". The HLR may additionally skip the procedures Update_Routing_Info and Control_Tracing_HLR if this indication is received from the VLR.

Sheet 2: If the HLR supports the Administrative Restriction of Subscribers Access feature and roaming is allowed in the VPLMN then the HLR may check the "Supported RAT Types" received from the VLR against the access restriction parameters. If this check fails then the decision box "Roaming allowed in this PLMN" shall take the exit "No".

Sheet 2: If the HLR supports MSISDN-less subscriptions and the subscriber's subscription is MSISDN-less, the test "Subscriber Allowed to Roam into PLMN?" takes the "no" exit e.g. if the VLR is known not to support MSISDN-less operation (see clause 3.6.1.5).

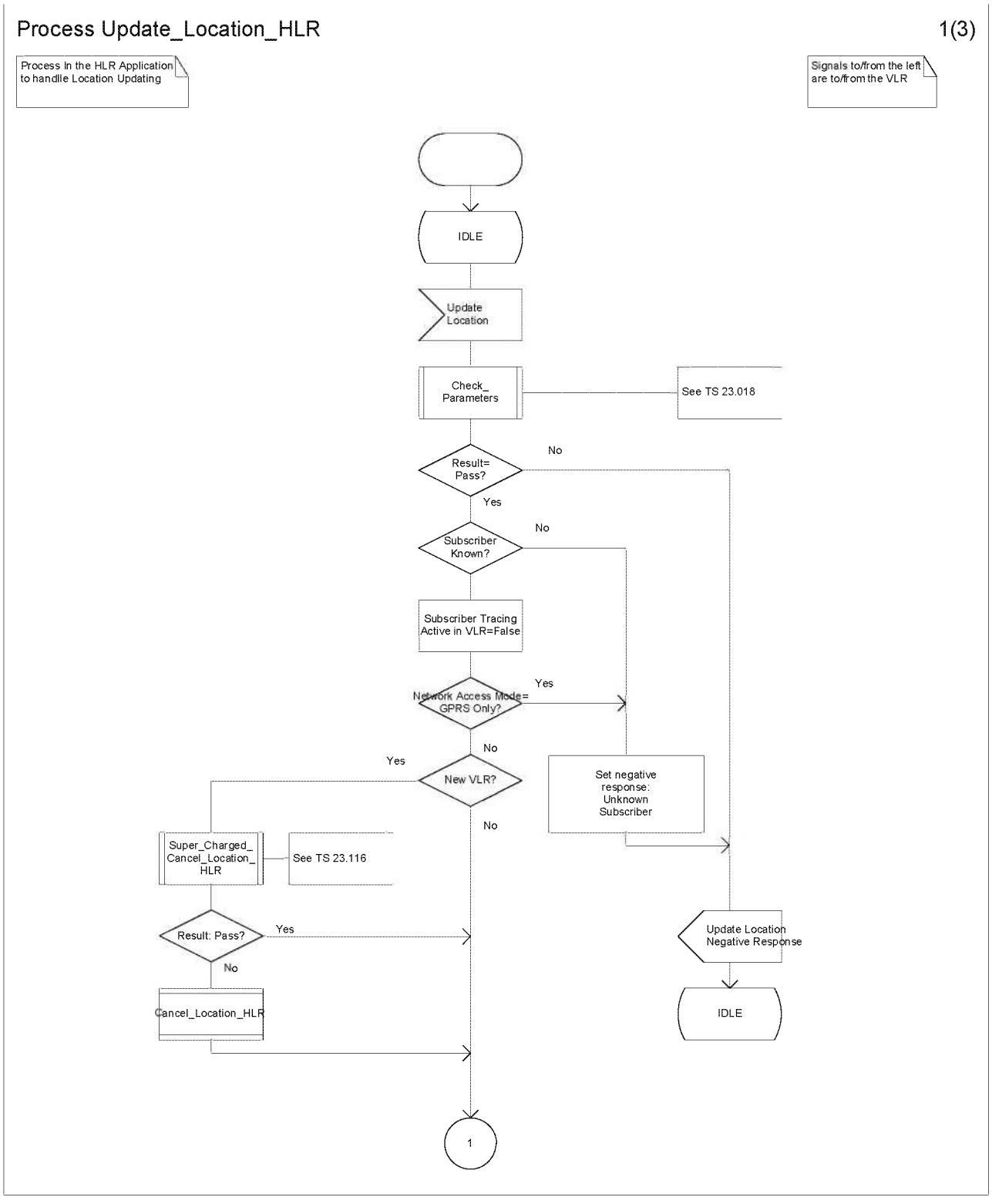

Figure 4.1.3.1 (sheet 1 of 3): Process Update_Location_HLR

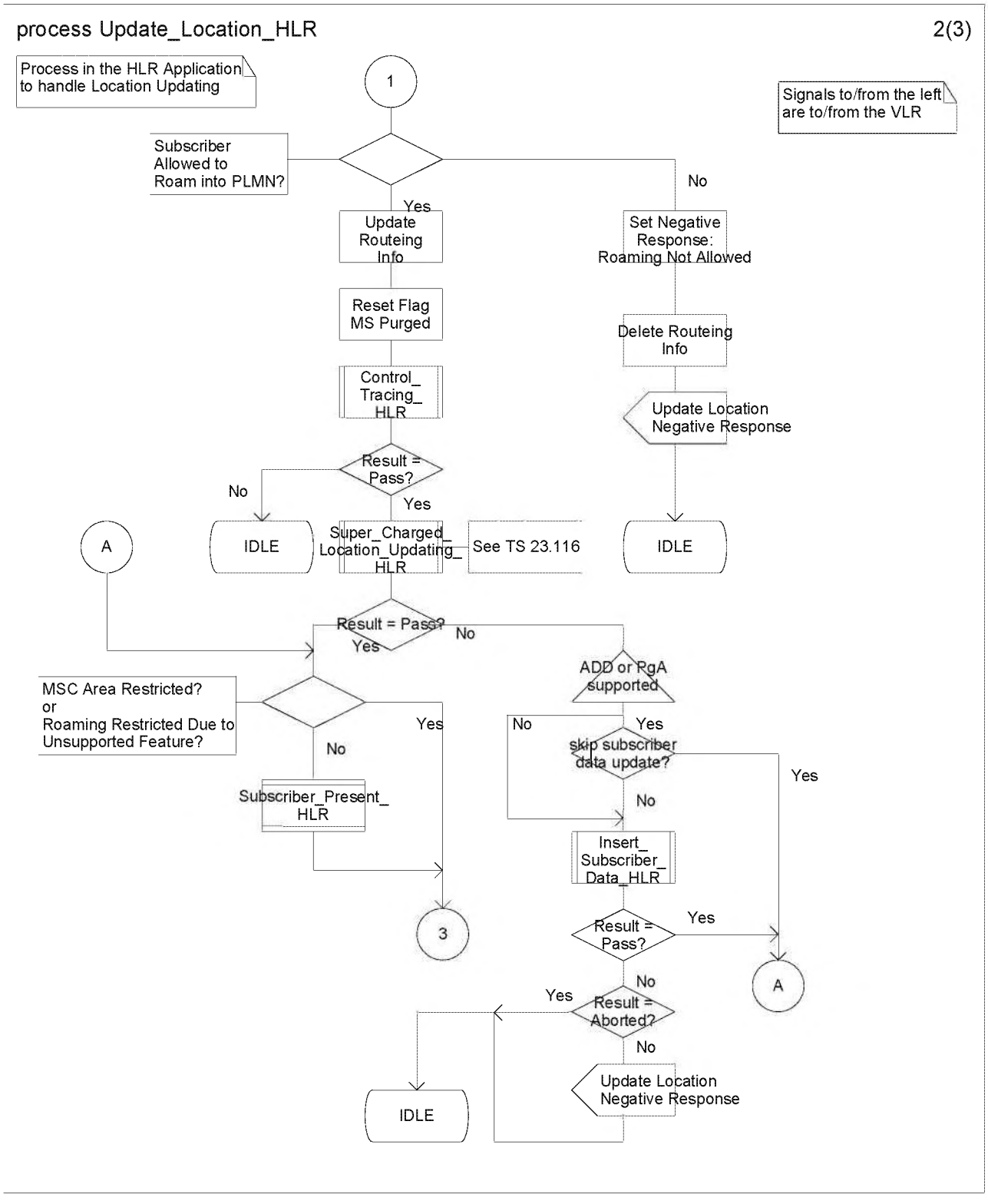

Figure 4.1.3.1 (sheet 2 of 3): Process Update_Location_HLR

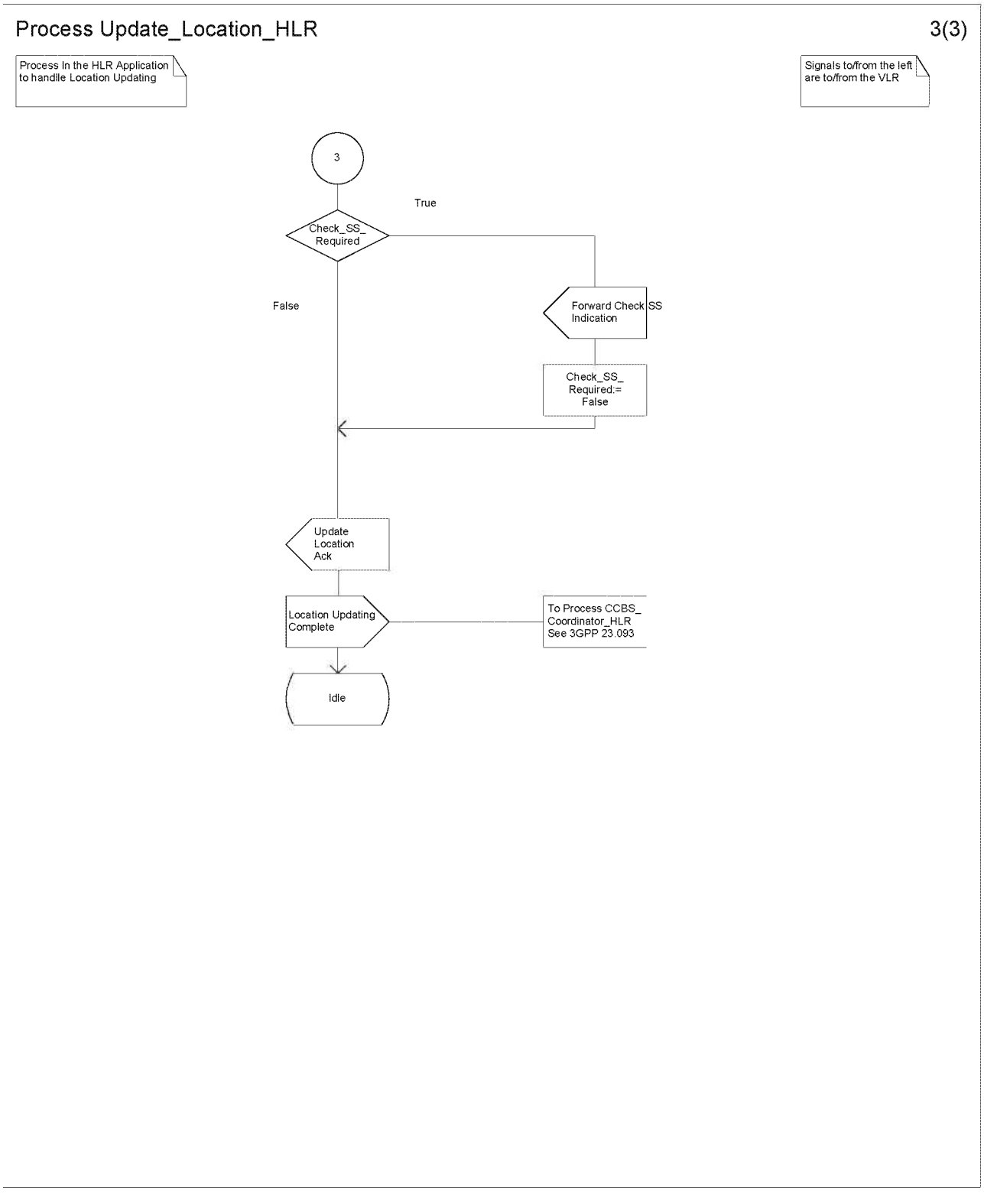

Figure 4.1.3.1 (sheet 3 of 3): Process Update_Location_HLR

4.1.3.2 Procedure Insert_Subscriber_Data_HLR

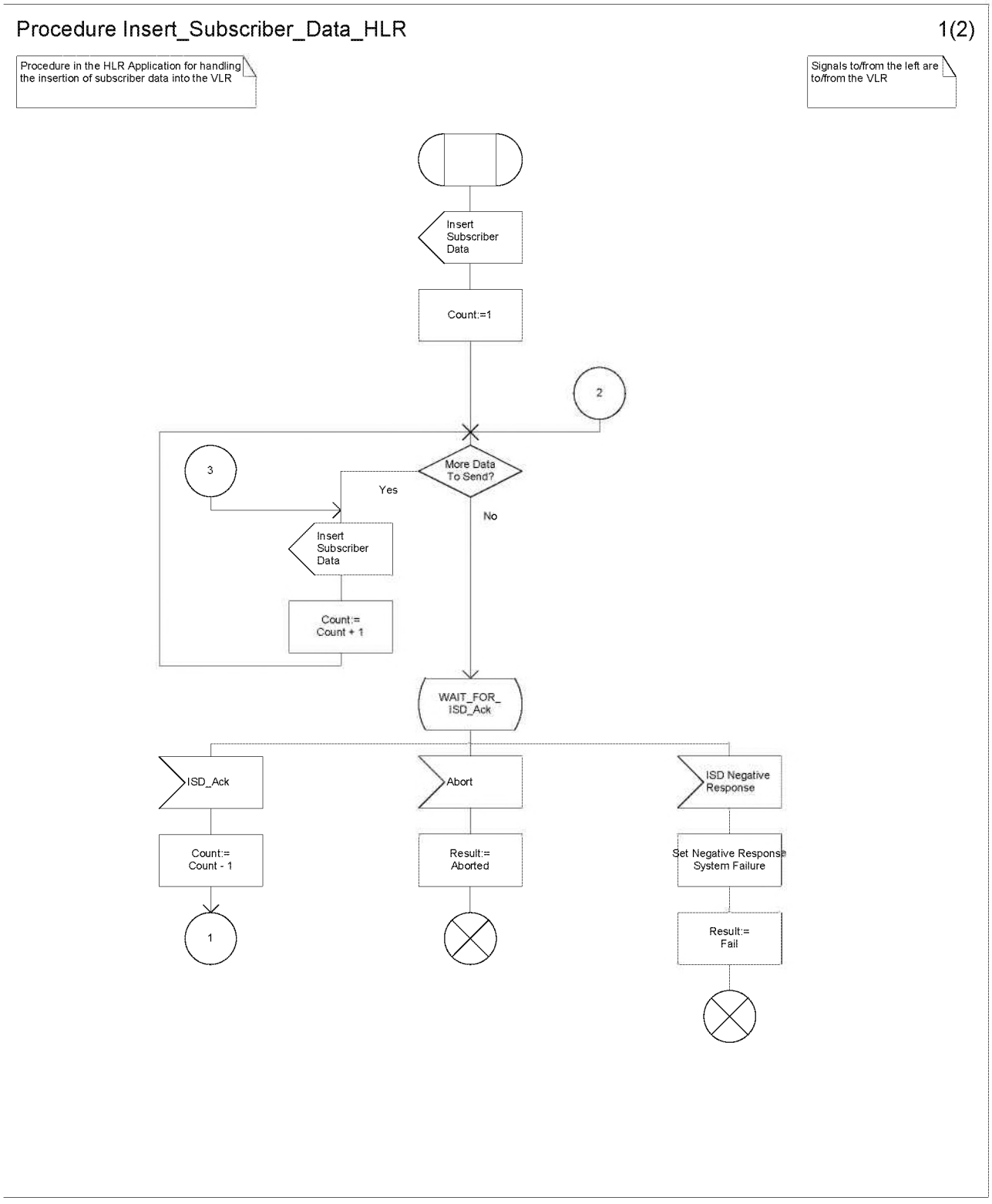

Figure 4.1.3.2 (sheet 1 of 2): Procedure Insert_Subscriber_Data_HLR

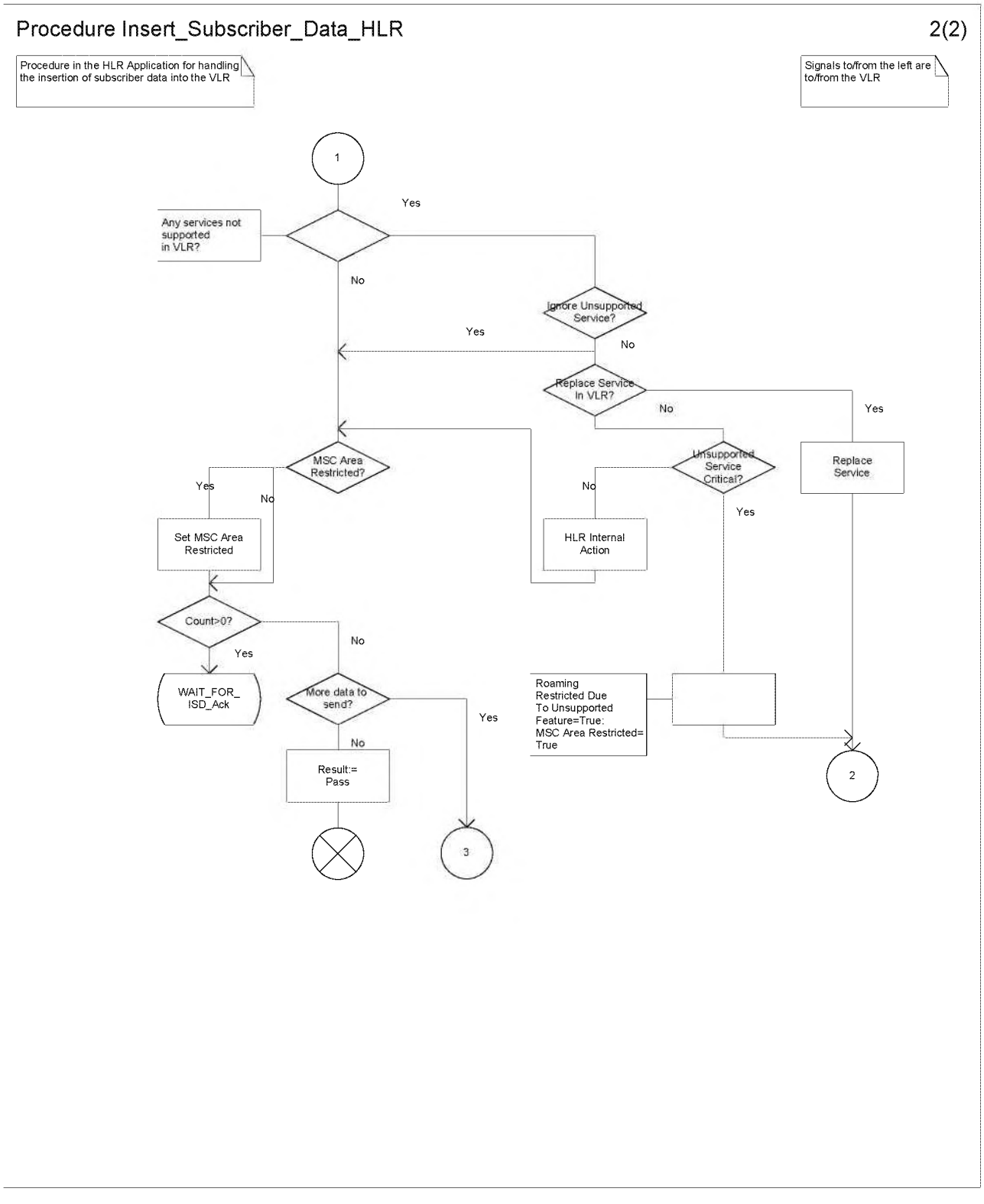

Figure 4.1.3.2 (sheet 2 of 2): Procedure Insert_Subscriber_Data_HLR

4.1.3.3 Process Subscriber_Present_HLR

The macro Alert_Service_Centre_HLR is specified in 3GPP TS 29.002 [8].

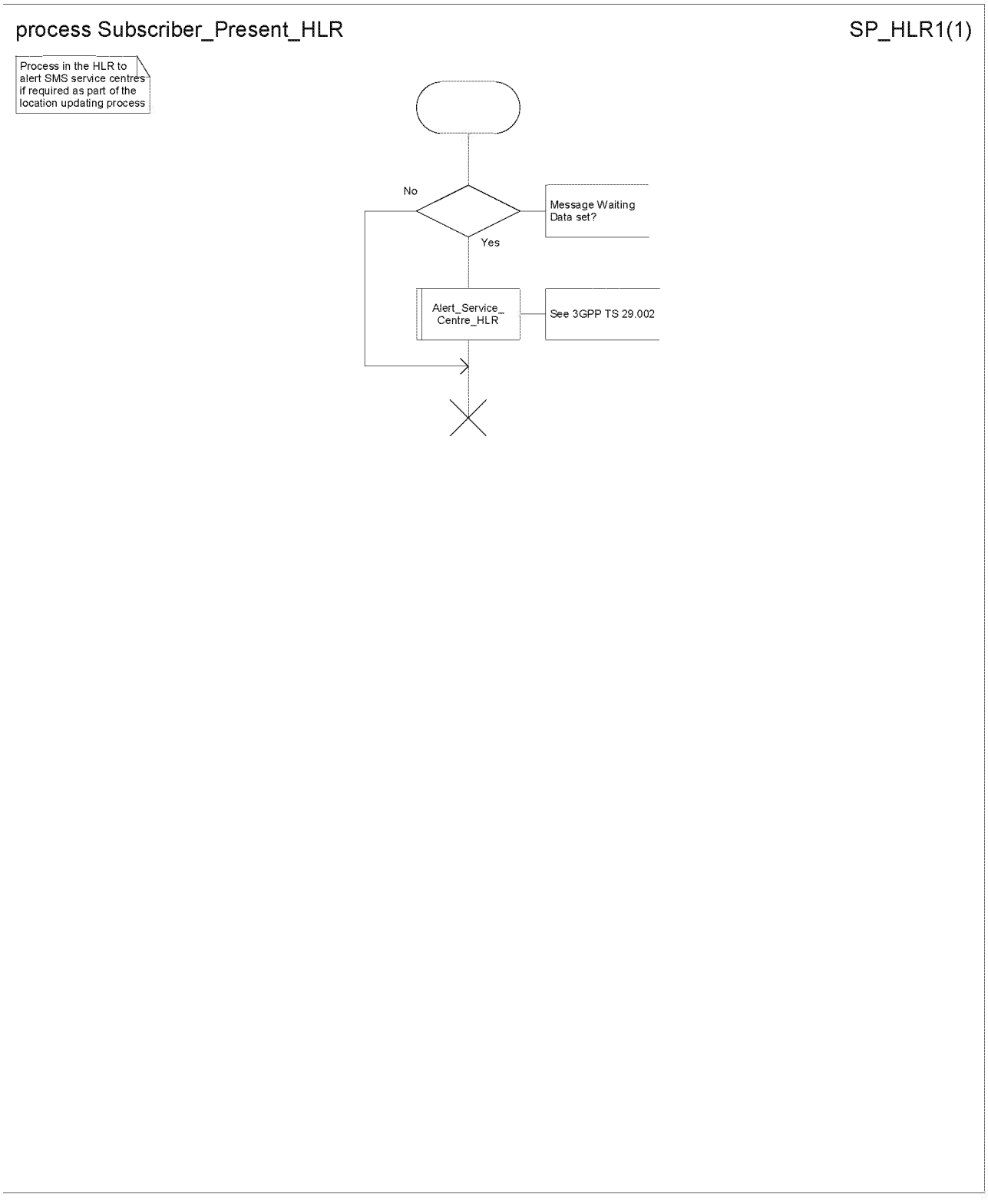

Figure 4.1.3.3: Process Subscriber_Present_HLR

4.1.3.4 Procedure Control_Tracing_HLR

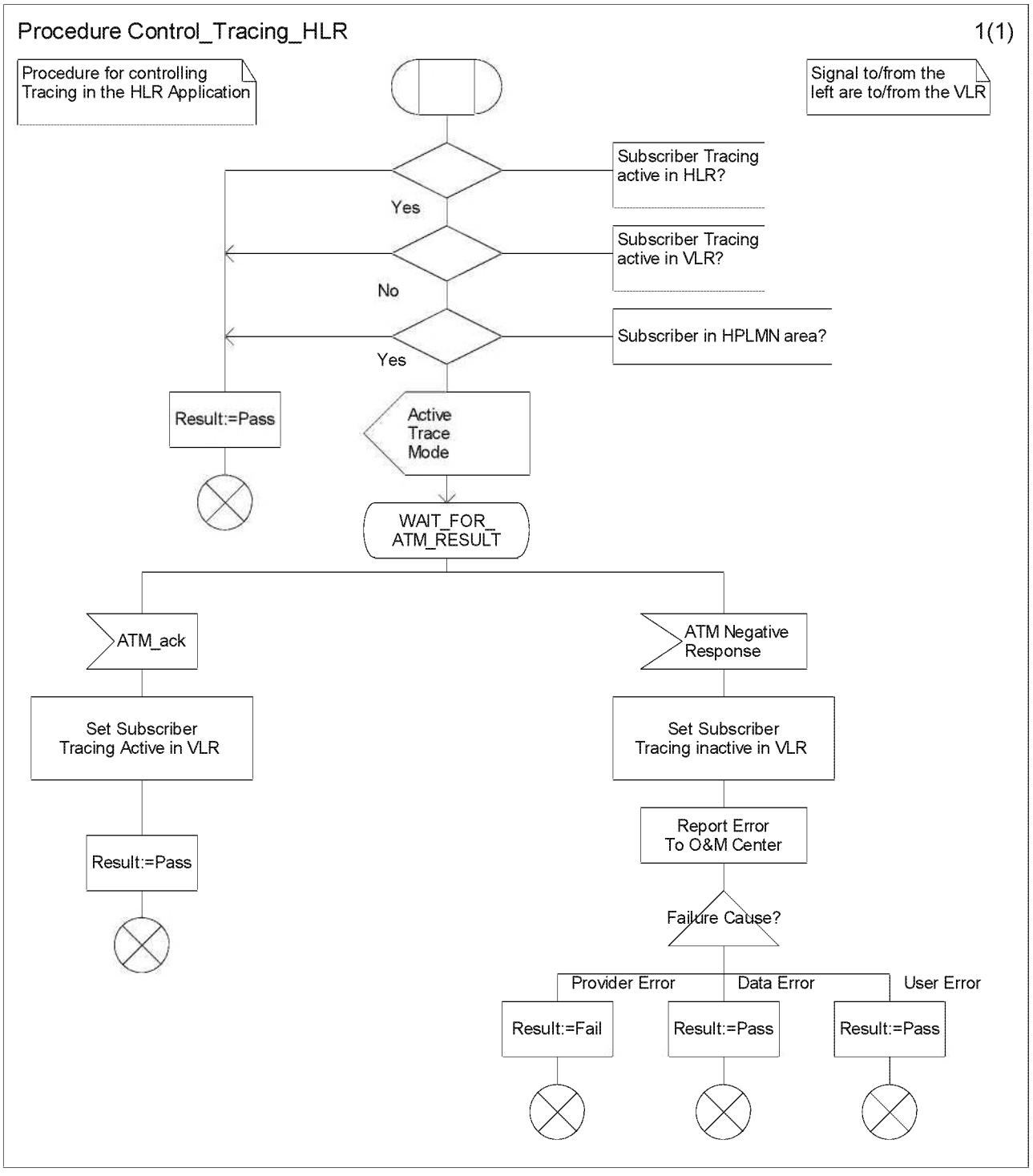

Figure 4.1.3.4 (sheet 1 of 1): Procedure Control_Tracing_HLR

4.1.4 Detailed procedure in the CSS

4.1.4.1 Process Update_VCSG_Location_CSS

The Update_VCSG_Location_CSS process takes place when the VLR needs to register the MS with the CSS and retrieve the CSG Subscription Data of the MS from the CSS.

The CSS receives an Update VCSG Location Request from the VLR.

If the MS is unknown in the CSS, and if the CSS supports creating the temporary empty subscription data for the MS, the CSS should create subscription data and sends successful update VCSG Location ACK message, otherwise the CSS shall sends a negative Update VCSG Location response message.

If the MS is known in the CSS, the CSS stores the received VLR number and initiates the Process Insert_VCSG_Subs_Data _CSS and at the end of the process acknowledges the Update VCSG Location request by sending an Update VCSG Location ACK message to the VLR.

Process Update_VCSG_Location_CSS

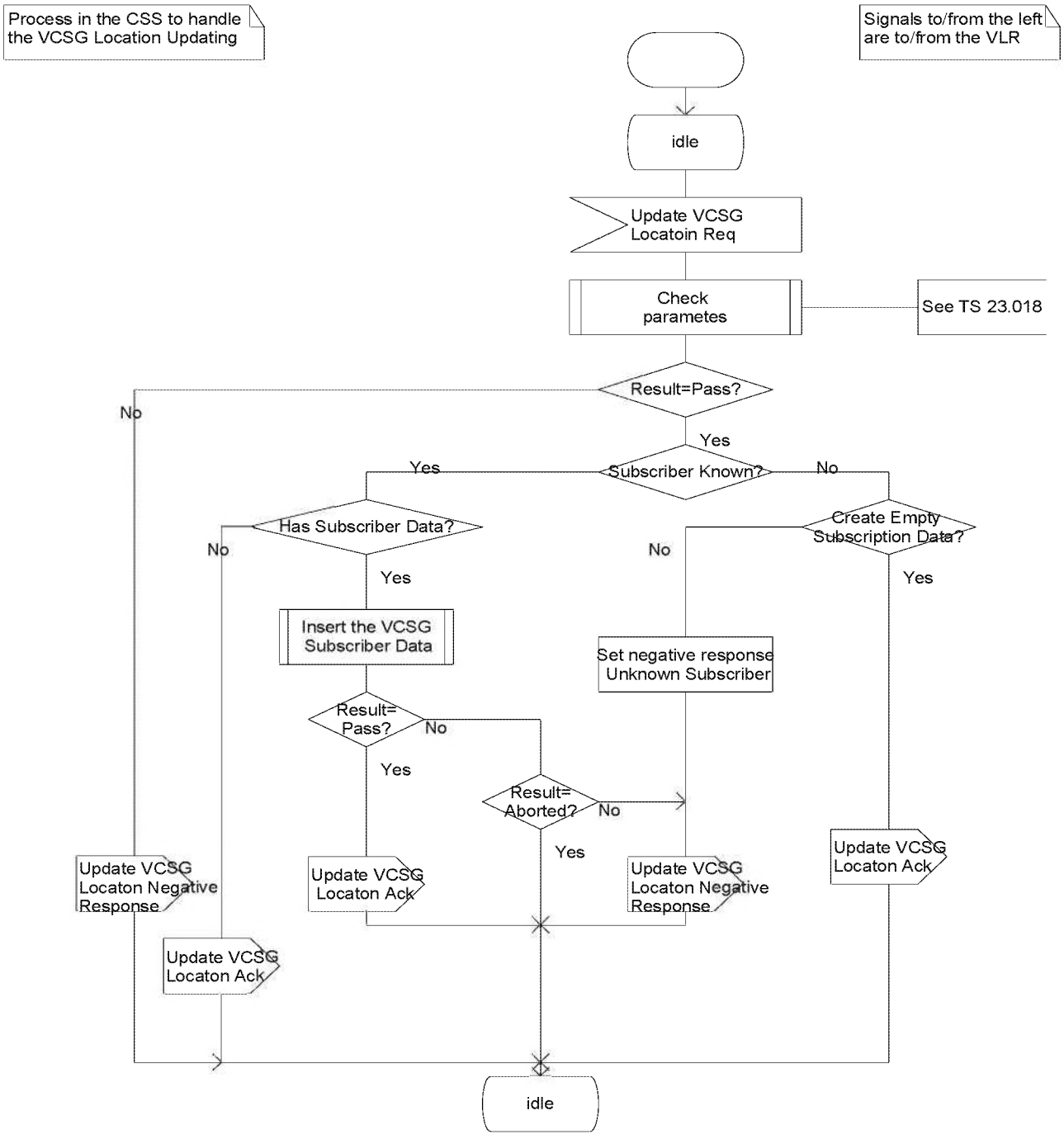

Figure 4.1.4.1 (sheet 1 of 1): Process Update_VCSG_Location_CSS

4.1.4.2 Procedure Insert_VCSG_Subs_Data_CSS

Whenever the CSG subscription data is changed for a MS in the CSS, and the changes affect the CSG subscription data stored in the VLR, the CSS initiates the Procedure Insert_VCSG_Subs_Data_CSS.

The Procedure Insert_VCSG_Subs_Data_CSS is also triggered by the Update_VCSG_Location_CSS process as specified in subclause 4.1.4.1.

When executing this procedure, the CSS sends an Insert VCSG Subscriber Data Request containing the CSG Subscription Data of the MS to the VLR and waits for the response from the VLR.

If the VLR successfully updates the received CSG Subscription Data from the CSS, it acknowledges the Insert VCSG Subscriber Data Request by returning an Insert VCSG Subscriber Data Ack. The CSS may wait for each request to be acknowledged before it ends the procedure.

If the CSS receives a negative response from the VLR, it sets the result with failure cause and ends this procedure.

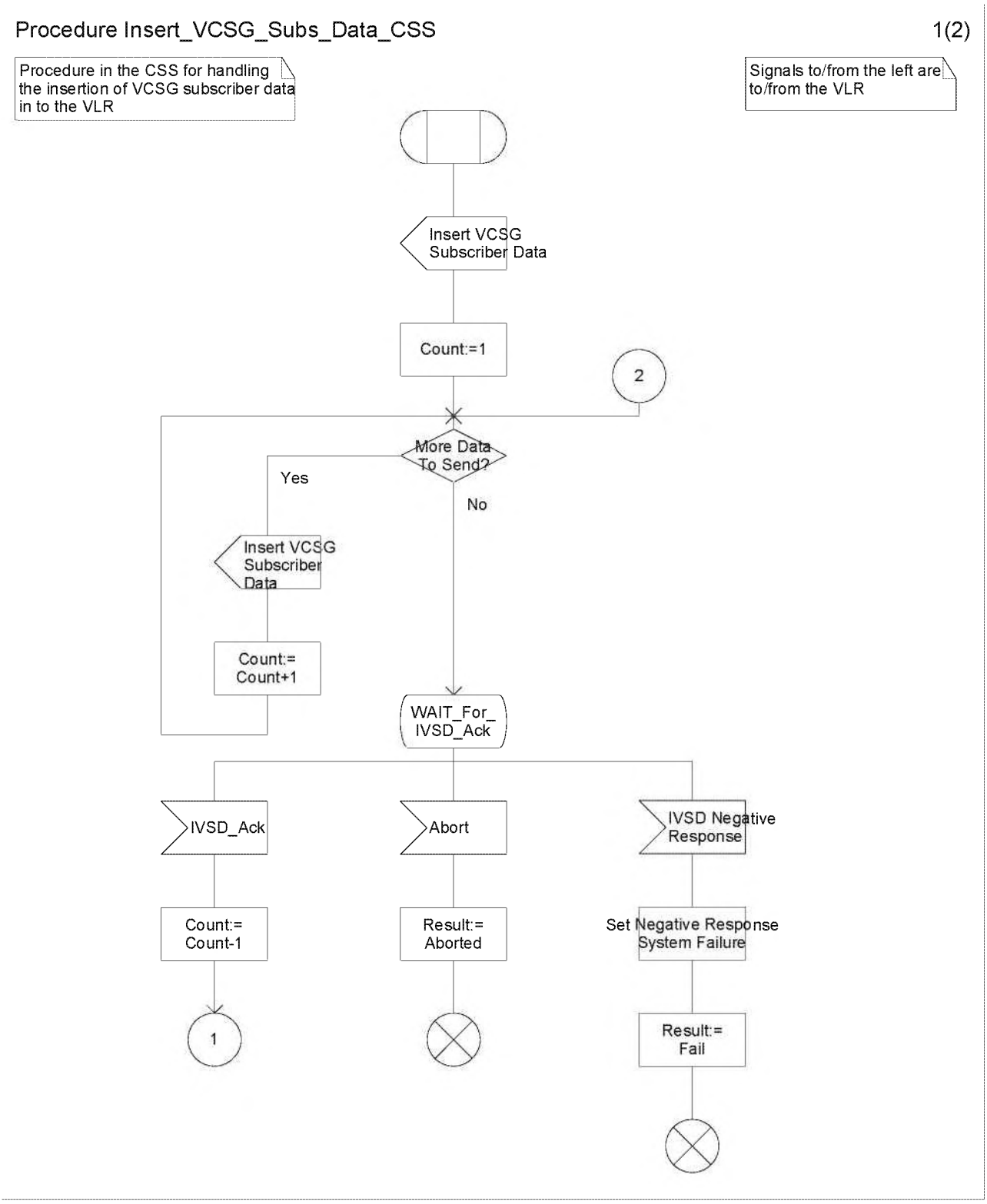

Figure 4.1.4.2 (sheet 1 of 2): Procedure Insert_VCSG_Subs_Data_CSS

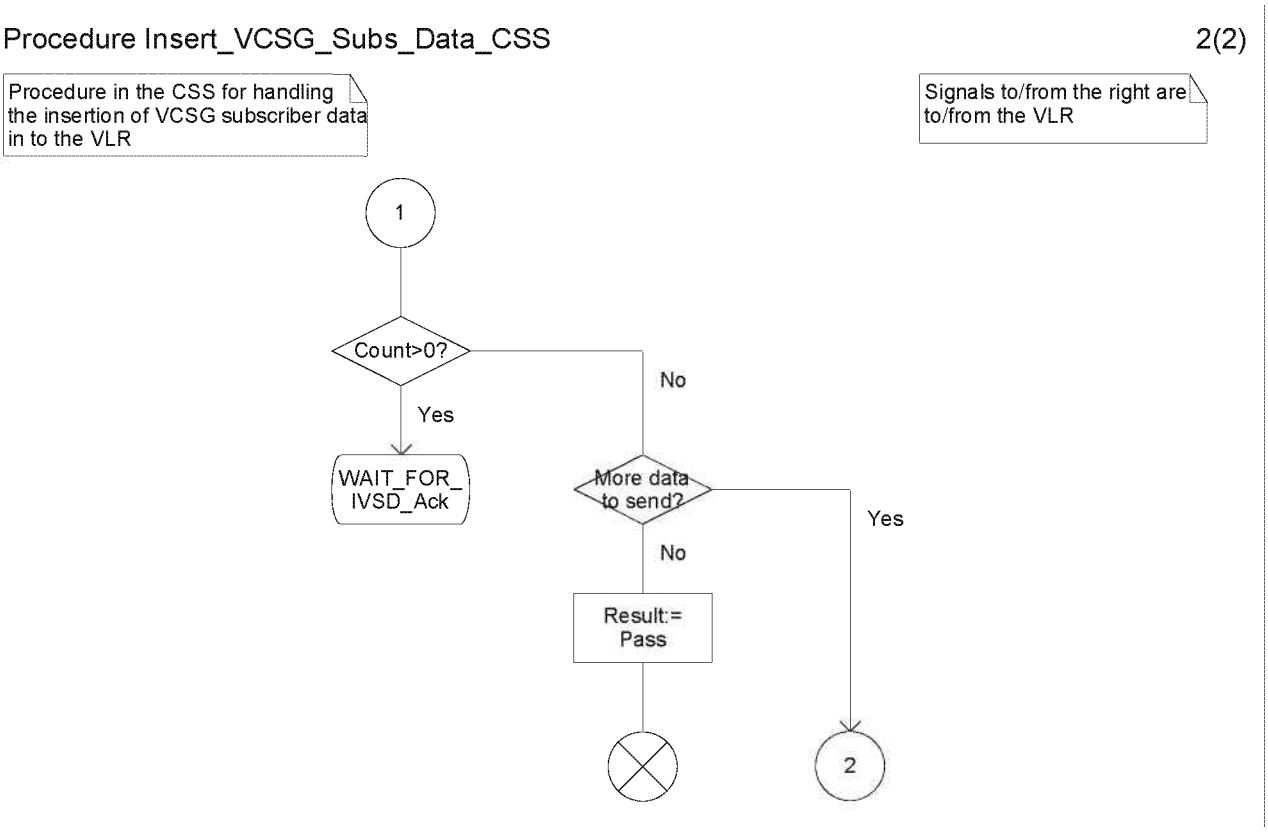

Figure 4.1.4.2 (sheet 2 of 2): Procedure Insert_VCSG_Subs_Data_CSS

4.2 Location Cancellation

4.2.1 Detailed procedure in the VLR

4.2.1.1 Process Cancel_Location_VLR

The procedure Check_Parameters is specified in 3GPP TS 23.018 [5a].

Sheet 1: If supported by the VLR, the "Subscriber data dormant" flag shall be set to true to allow triggering Mobile Terminating Roaming Retry. A VLR not supporting this flag shall behave as if the flag is set to false.

Sheet 1: A VLR not supporting the Mobile Terminating Roaming Retry feature and the Mobile Terminating Roaming Forwarding fearture (see 3GPP TS 23.018 [5a]) may not send Cancel Location to MSC.

Sheet 1: A VLR supporting the Mobile Terminating Roaming Retry feature sets the "Cancel Location received" flag to true when receiving the Cancel Location message from the HLR. This is used to determine whether to trigger MT roaming retry upon receipt of an incoming call, see subclause 7.3.2.1 of 3GPP TS 23.018 [5a].

Sheet 1: A VLR supporting the Mobile Terminating Roaming Forwarding feature may include the MTRF Supported And Authorized flag or the MTRF Supported And Not Authorized flag in the Cancel Location message it sends to the MSC if received in the Cancel Location message from the HLR.

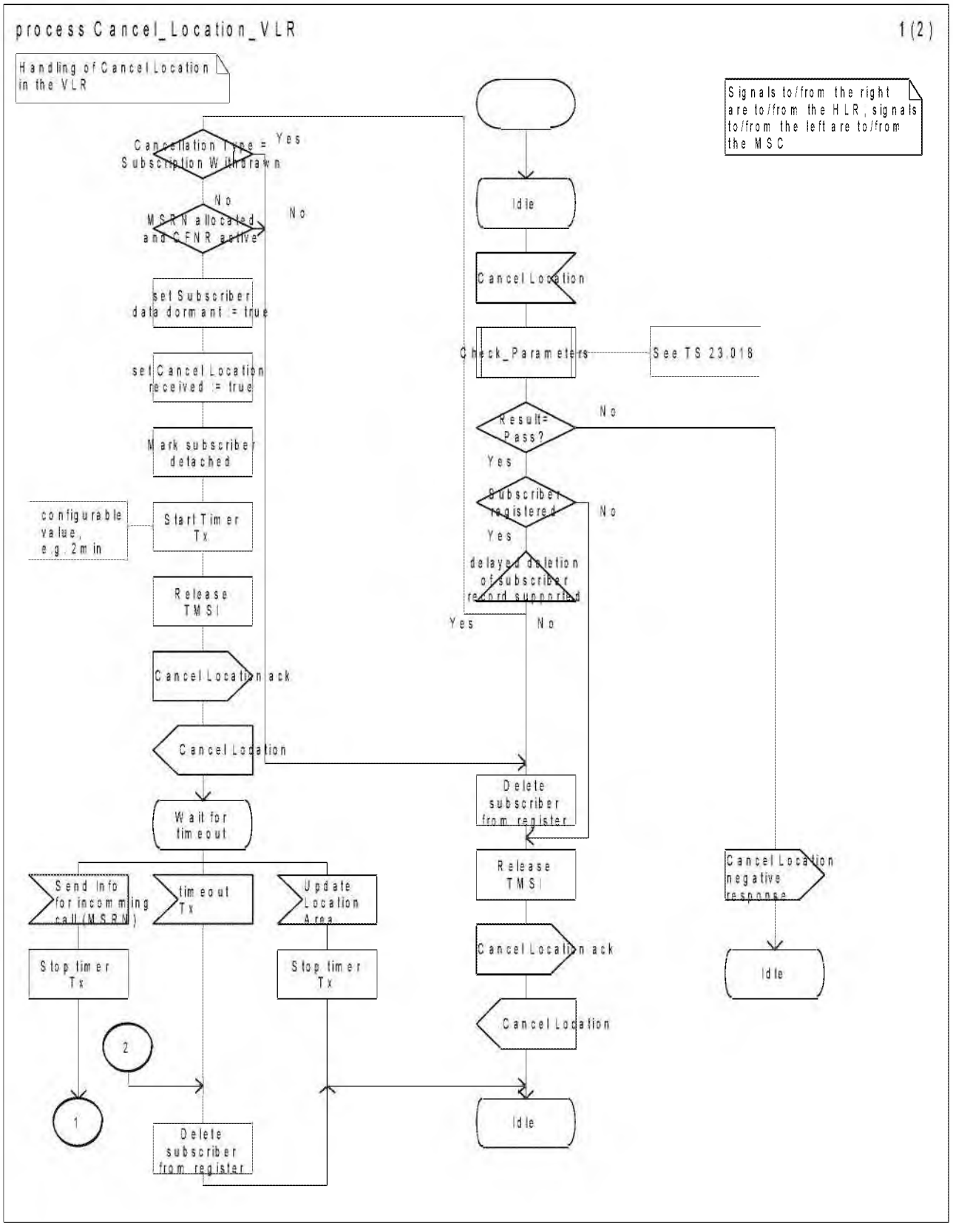

Figure 4.2.1.1 (Sheet 1 of 2): Process Cancel_Location_VLR

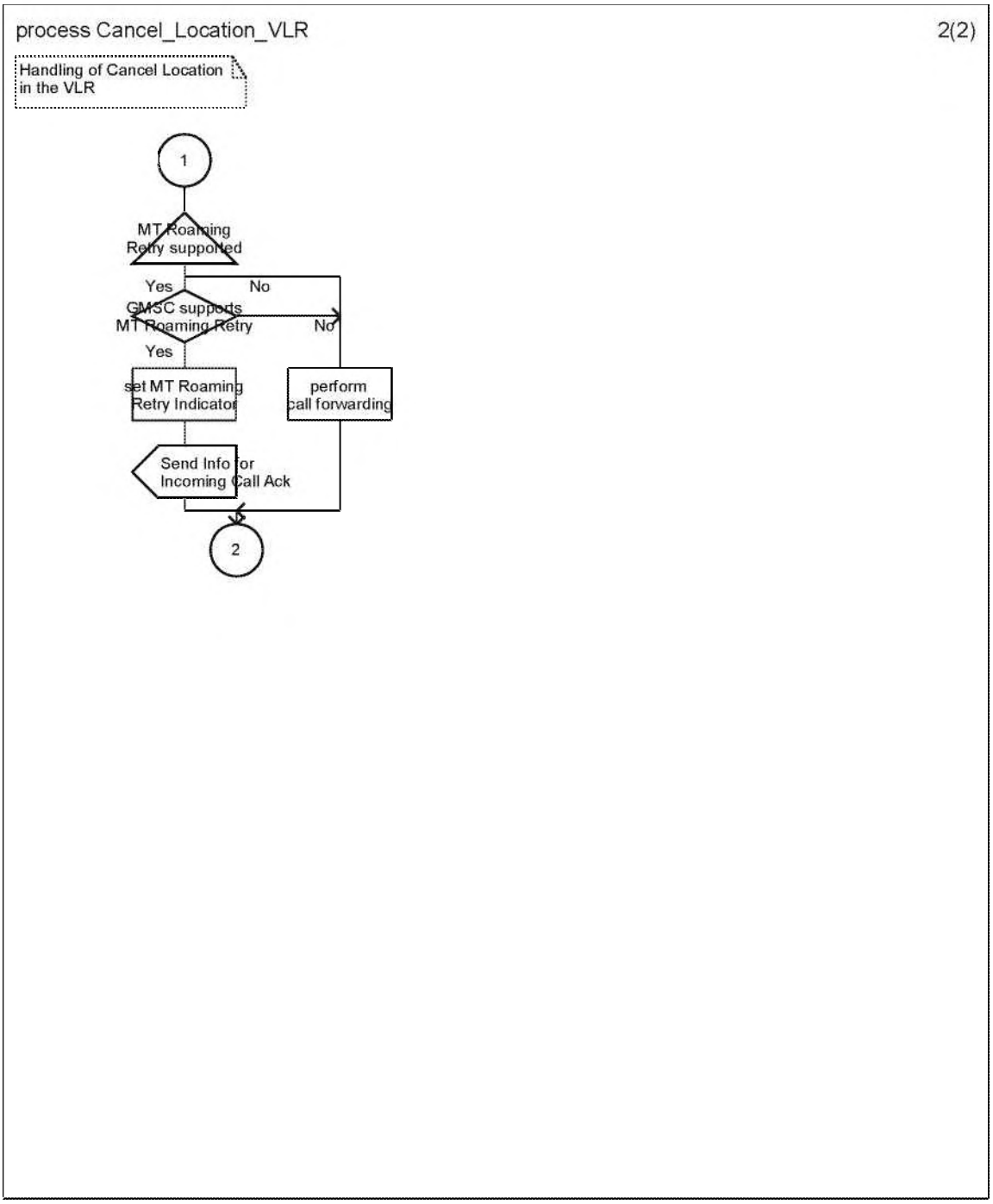

Figure 4.2.1.1 (Sheet 2 of 2): Process Cancel_Location_VLR

4.2.2 Detailed procedure in the HLR

4.2.2.1 Process Cancel_Location_HLR

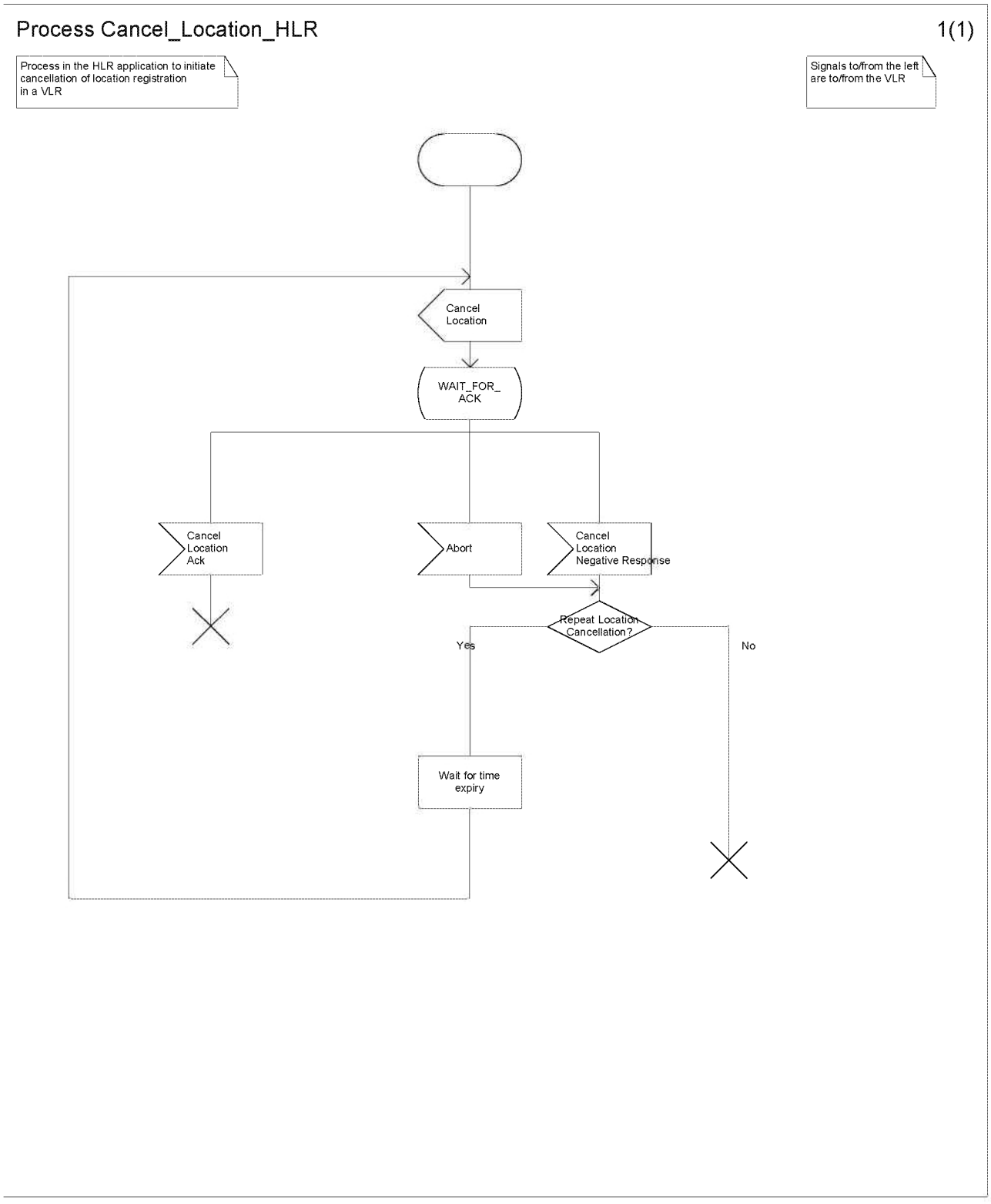

Figure 4.2.2.1: Process Cancel_Location_HLR

4.2A VCSG Location Cancellation

4.2A.1 Detailed procedure in the VLR

4.2A.1.1 Process Cancel_VCSG Location_VLR

The procedure Check_Parameters is specified in 3GPP TS 23.018 [5a].

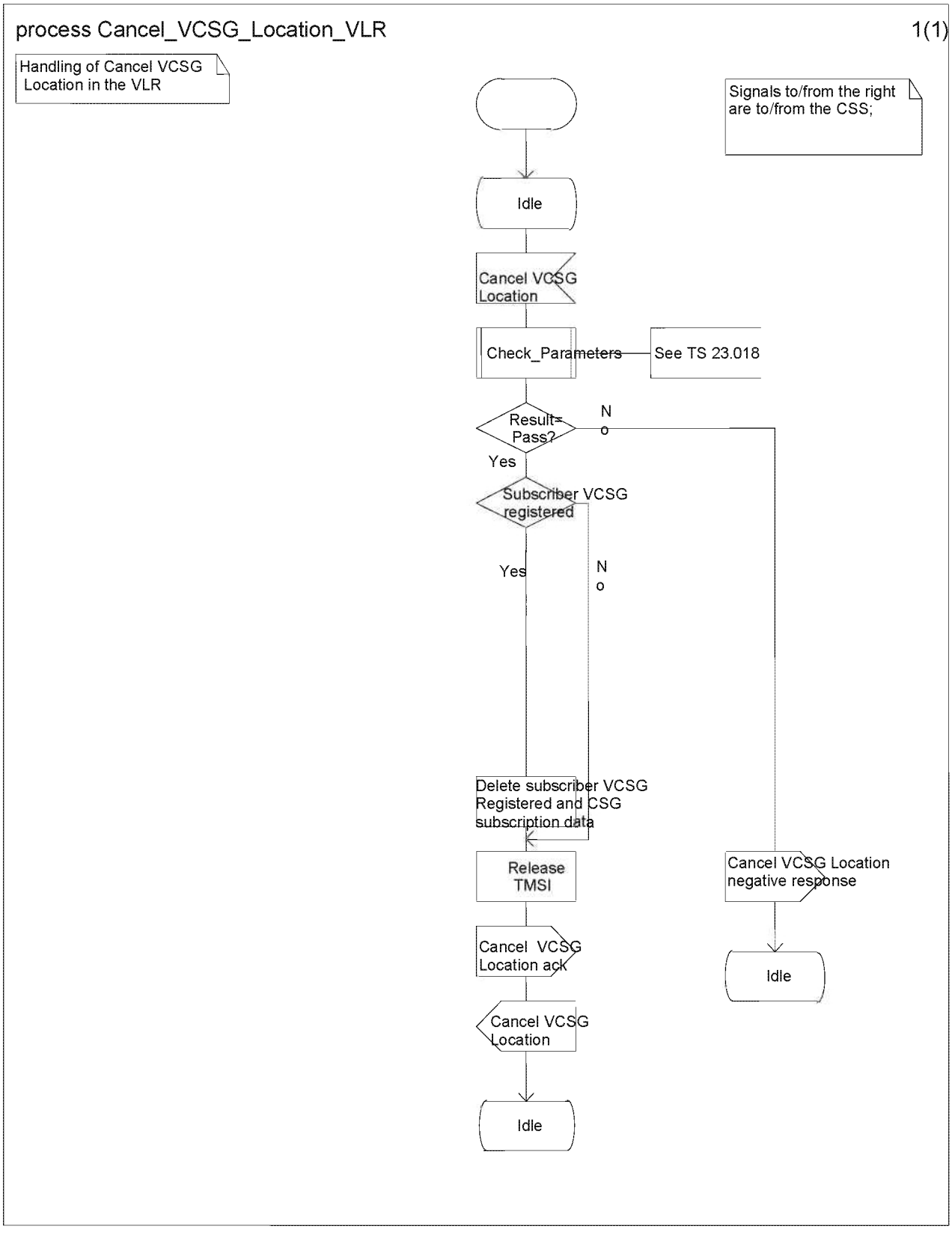

Figure 4.2A.1.1 (Sheet 1 of 1): Process Cancel_VCSG_Location_VLR

4.2A.2 Detailed procedure in the CSS

4.2A.2.1 Process Cancel_VCSG Location

If the CSS determines to delete the registration of the MS which does not have the valid CSG subscription data, the CSS shall send the Cancel VCSG Location to the VLR.

NOTE: How the CSS determines when to remove the registration of the MS is implementation dependent.

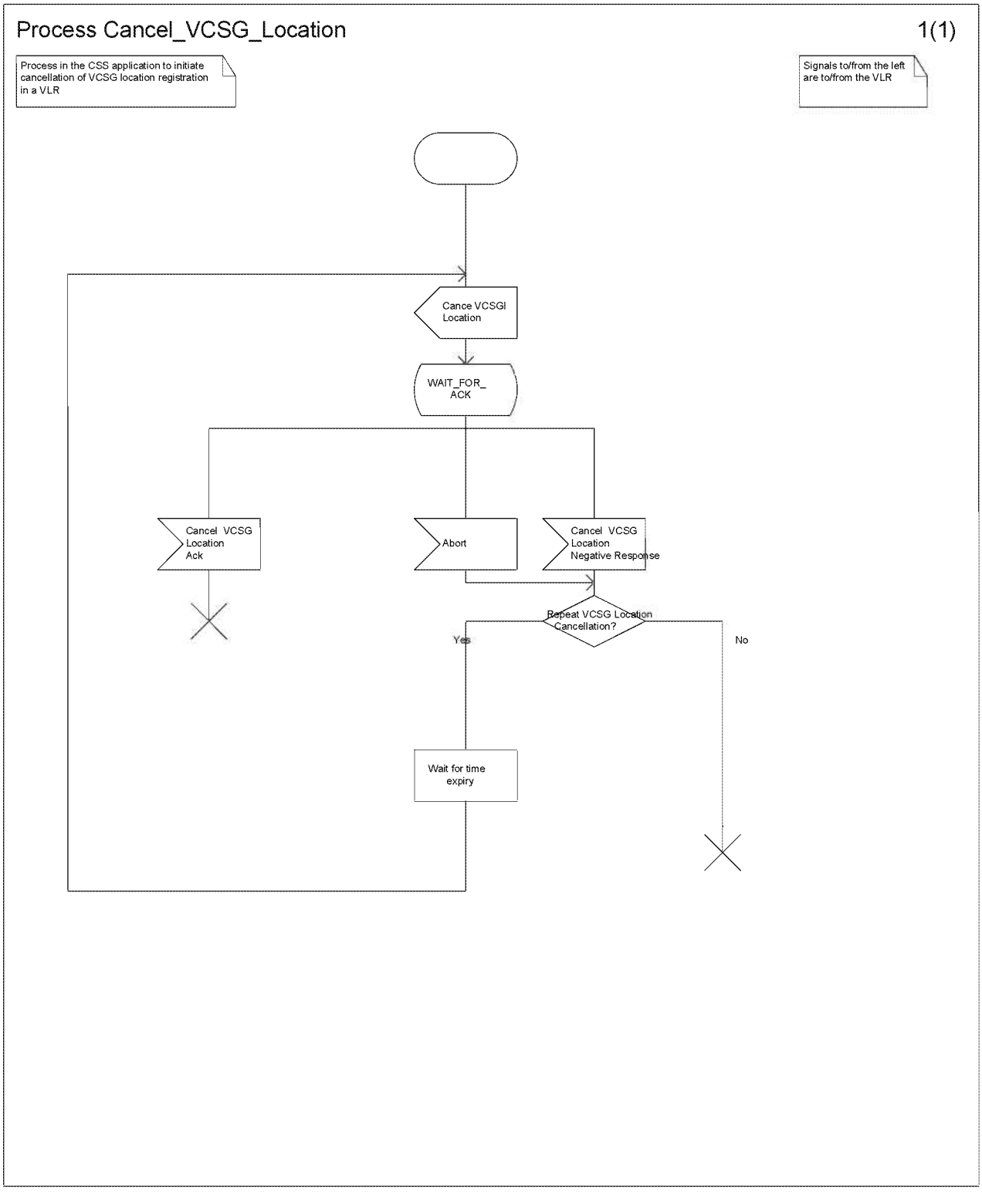

Figure 4.2A.2.1: Process Cancel_Location_CSS

4.3 Detach IMSI

4.3.1 Detailed procedure in the MSC

4.3.1.1 Process Detach_IMSI_MSC

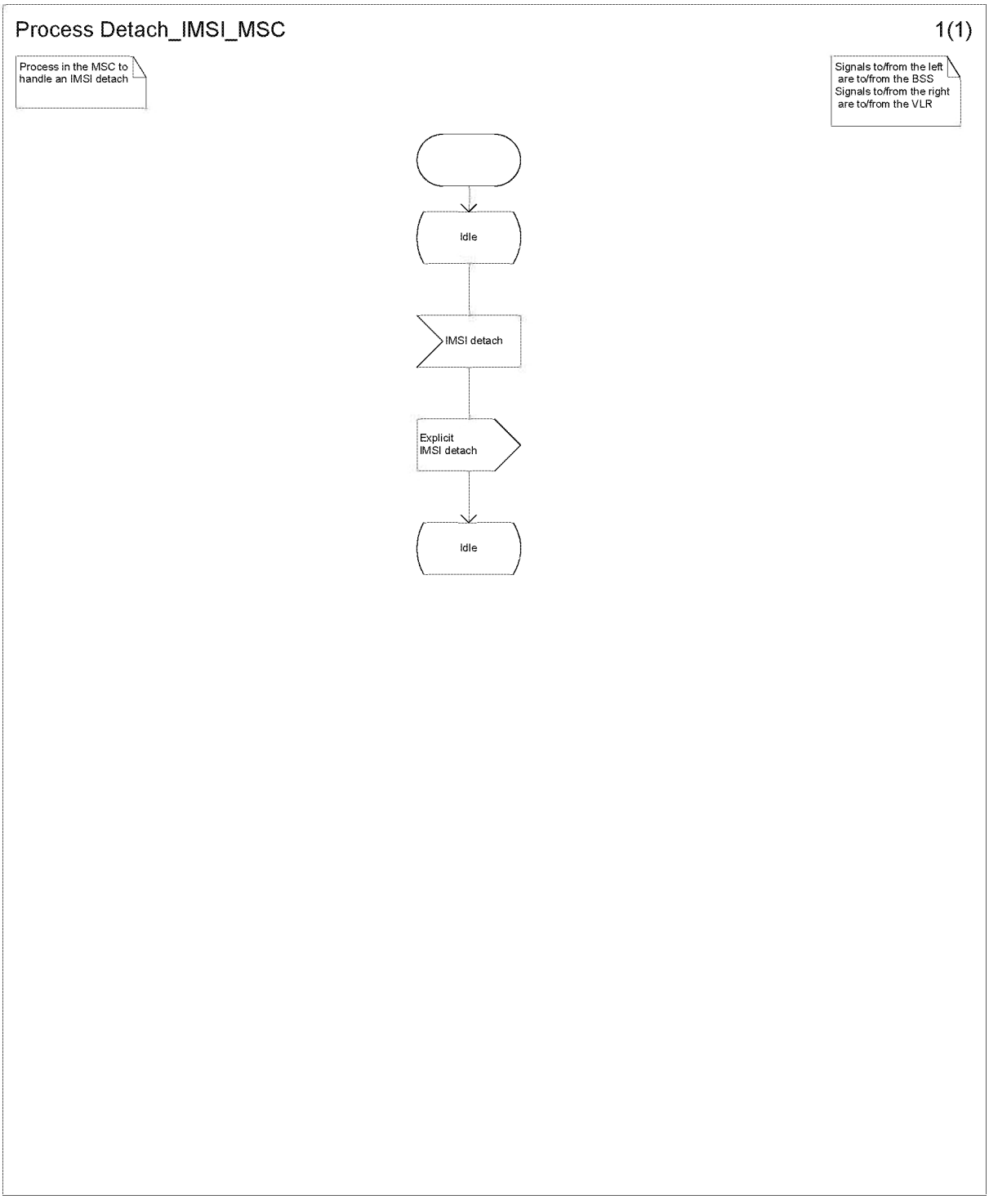

Figure 4.3.1.1 (Sheet 1 of 1): Process Detach_IMSI_MSC

4.3.2 Detailed procedure in the VLR

4.3.2.1 Process Detach_IMSI_VLR

The signal "Authenticated Radio Contact Terminated" is sent to Process Detach_IMSI_VLR from RR handling in the MSC whenever authenticated radio contact is terminated, e.g. at the release of a call.

The procedure "Notify_gsmSCF" is specified in 3GPP TS 23.078 [11]. The "Notify" parameter indicates whether the IMSI detach was explicit or implicit.

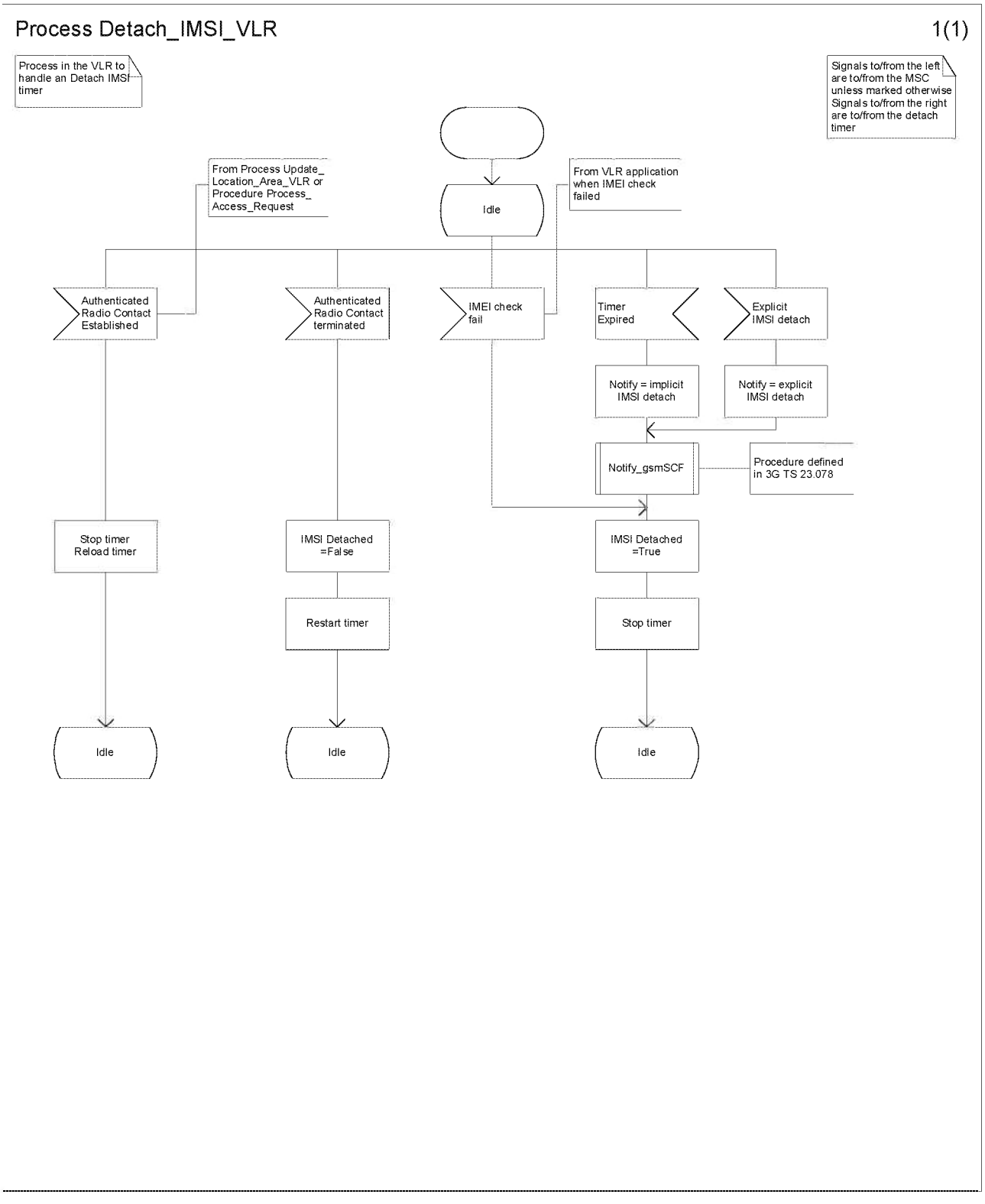

Figure 4.3.1.1 (Sheet 1 of 1): Process Detach_IMSI_VLR

4.4 Purge MS

4.4.1 Detailed procedure in the VLR

4.4.1.1 Procedure Purge_MS_VLR

Sheet 1: The procedure Purge_MS_In_Serving_Network_Entity is specific to Super-Charger; it is specified in 3GPP TS 23.116 [7]. If the VLR and the originating HLR support the Super-Charger functionality, processing continues from the "Yes" exit of the test "Result=Pass?".

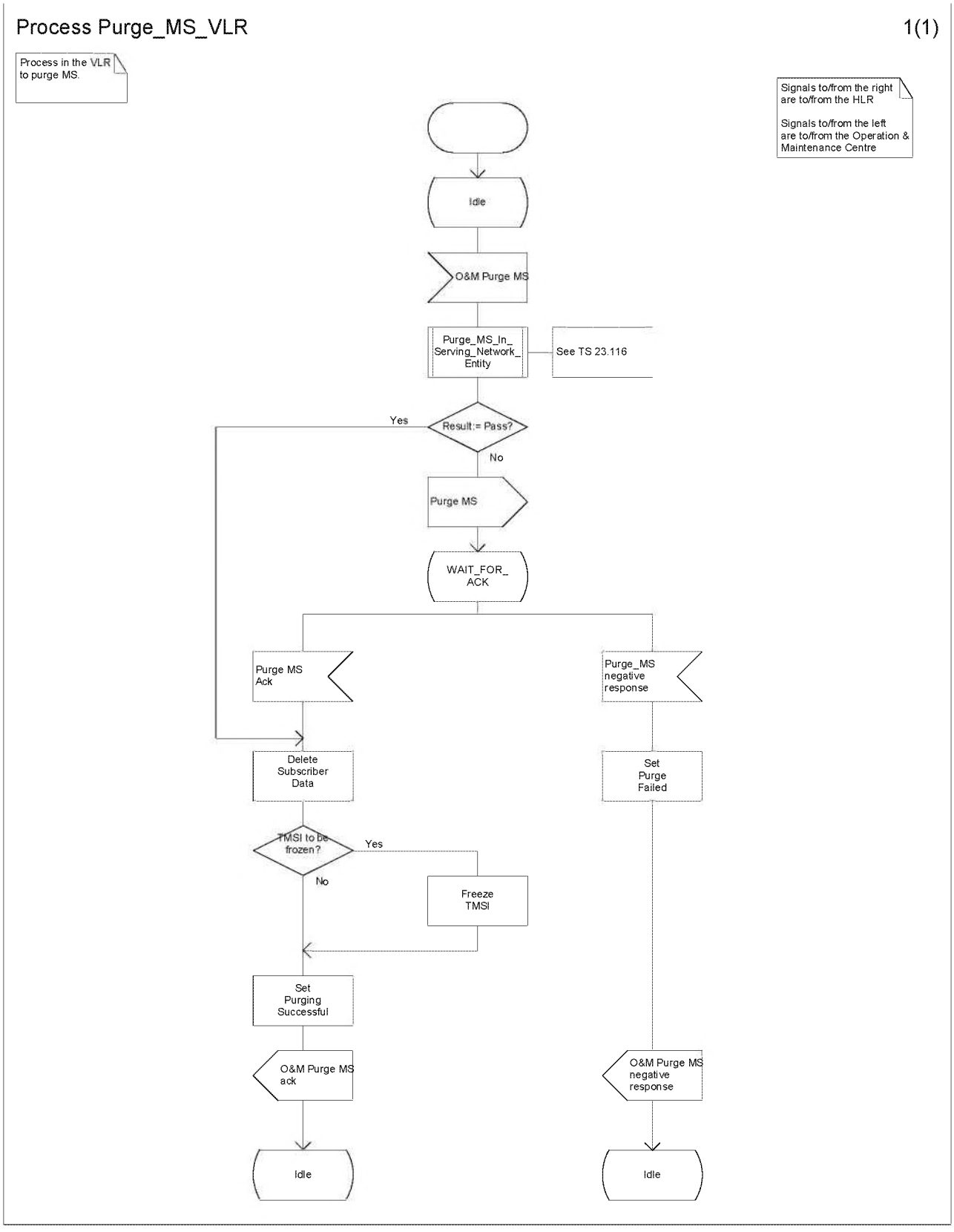

Figure 4.4.1.1 (Sheet 1 of 1): Procedure Purge_MS_VLR

4.4.2 Detailed procedure in the HLR

4.4.2.1 Process Purge_MS_HLR

The procedure Check_Parameters is specified in 3GPP TS 23.018 [5a].

If the received VLR number and the stored VLR number do not match, the HLR sends Purge MS ack containing an empty result to indicate successful outcome. Since the MS is known by the HLR to be in a different VLR area, it is not appropriate to block mobile terminated calls or short messages to the MS, but the VLR which initiated the purging procedure can safely purge its record for the MS without freezing the TMSI.

If the received SGSN number and the stored SGSN number do not match, the HLR sends a Purge MS ack containing an empty result to indicate successful outcome. Since the MS is known by the HLR to be in a different SGSN area, it is not appropriate to block short messages to the MS, but the SGSN which initiated the purging procedure can safely purge its record for the MS without freezing the P-TMSI.

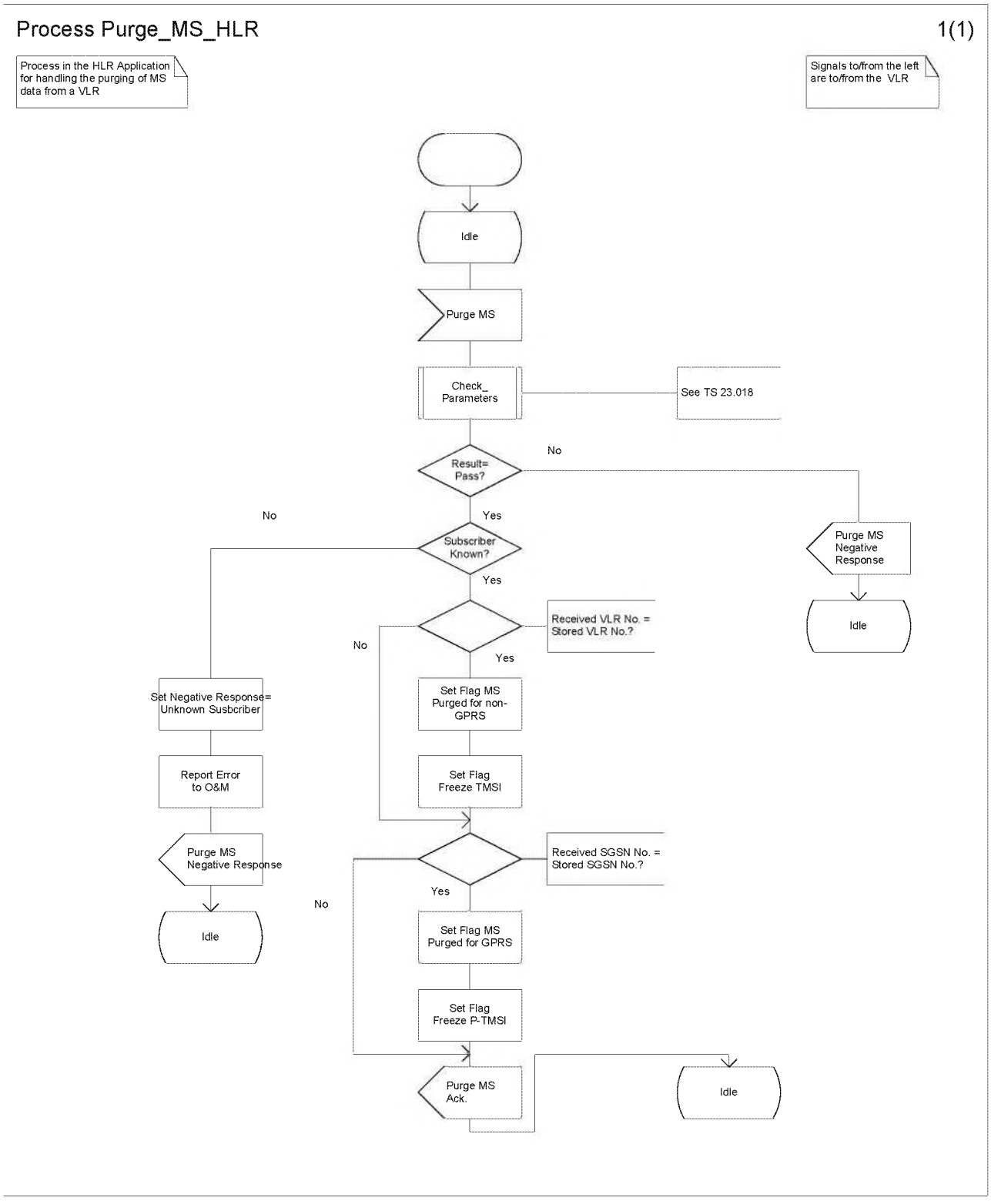

Figure 4.4.2.1 (Sheet 1 of 1): Procedure Purge_MS_HLR

Annex A (informative): Change history

Change history						
TSG CN#	Spec	Version	CR	<Phase>	New Version	Subject/Comment
Apr 1999	GSM 03.12	6.0.0				Transferred to 3GPP CN1
CN#03	23.012				3.0.0	Approved at CN#03
CN#06	23.012	3.0.0	001r1	R99	3.1.0	Restructuring of MAP Location Management Procedures, Stage 2
CN#06	23.012	3.0.0	002	R99	3.1.0	Introduction of Super-Charger into TS 23.012
CN#07	23.012	3.1.0	003r3	R99	3.2.0	Introduction of Enhanced User Identity Confidentiality
CN#07	23.012	3.1.0	004	R99	3.2.0	Addition of Current Security Context Data to Send_Identification_PVLR
CN#07	23.012	3.1.0	005	R99	3.2.0	Introduction of Authentication Failure Report
	23.012	3.2.0		R99	3.2.1	CR 23.012-003r3 removed because implemented in error
CN#08	23.012	3.2.1	006	R99	3.3.0	Introduction of Mobility Management event notification into 23.012 procedures
CN#11	23.012	3.3.0		Rel-4	4.0.0	Release 4 after CN#11
CN#11	23.012	4.0.0	008r1	Rel-5	5.0.0	Relaying of SendIdentification when IuFlex is applied
CN#20	23.012	5.0.0	010r1	Rel-5	5.1.0	Addition of procedure to retrieve UE-specific behaviour data
CN#21	23.012	5.1.0	012	Rel-5	5.2.0	Correction of misaligned signal names between VLR and PVLR
CN#21	23.012	5.1.0	013r1	Rel-5	5.2.0	Corrections to "Early UE" handling
CN#23	23.012	5.2.0	014r1	Rel-6	6.0.0	Include administrative restriction subscription parameter
CN#24	23.012	6.0.0	015r6	Rel-6	6.1.0	Addition of ADD feature
CN#25	23.012	6.2.0	016r1	Rel-6	6.2.0	Clarification of the Automatic Device Detection feature
CN#27	23.012	6.2.0	018r2	Rel-6	6.3.0	Introduction of Hop Counter for Send Identification
CN#27	23.012	6.2.0	018r2	Rel-6	6.3.0	Management Based Activation Impacts
CT#31	23.012	6.3.0	0020	Rel-7	7.0.0	Enhancement of the administrative restriction of subscribers' access feature
CT#32	23.012	7.0.0	0022	Rel-7	7.1.0	Use of cause #12 in VPLMNs
CT#32	23.012	7.0.0	0021	Rel-7	7.1.0	Skipping Update Location and Control Tracing for SkipSubscriberData
CT#34	23.012	7.1.0	0024r1	Rel-7	7.2.0	Change to CANCEL_LOCATION procedure in VLR
CT#36	23.012	7.2.0	0026r2	Rel-7	7.3.0	Mobile Termination whilst the MS is moving to another MSC
CT#40	23.012	7.3.0	0027r1	Rel-8	8.0.0	Paging optimization with A/Iu flex
CT#42	23.012	8.0.0	0029	Rel-8	8.1.0	TMSI re-allocation during Location Updating Reject with cause #13 or #15
CT#44	23.012	8.1.0	0030r1	Rel-8	8.2.0	MAP Update Location w/o the PgA parameter
CT#46	-	8.2.0	-		9.0.0	Update to Rel-9 version (MCC)
CT#49	23.012	9.0.0	0034r4	Rel-9	9.1.0	Correction to Tracing Control Handling Behaviour of HLR in CS Domain
CT#51	23.012	9.1.0	0035r1	Rel-10	10.0.0	MT Roaming Retry and Super Charger
CT#51	23.012	9.1.0	0036r1	Rel-10	10.0.0	Mobile Terminating Roaming Forwarding
CT#52	23.012	10.0.0	0037r1	Rel-10	10.1.0	Periodic LAU timer in HSS subscription
CT#52	23.012	10.0.0	0038r2	Rel-10	10.1.0	Inclusion of congestion control and back-off timer for CS attach requests
CT#56	23.012	10.1.0	0040r2	Rel-11	11.0.0	Retrieval of VPLMN CSG subscription information for CS domain
CT#57	23.012	11.0.0	0041r1	Rel-11	11.1.0	Cancel VCSG Location
CT#57	23.012	11.0.0	0042r2	Rel-11	11.1.0	Temporary empty CSG subscription data Indicator
CT#57	23.012	11.0.0	0043r1	Rel-11	11.1.0	Support for MSC in Pool to avoid dual VLR registration

Change history						
TSG CN#	Spec	Version	CR	<Phase>	New Version	Subject/Comment
	23.012	11.1.0		Rel-11	11.1.1	Missing SDLs added
CT#58	23.012	11.1.1	0044r2	Rel-11	11.2.0	MSISDN-less UEs
2014-09	23.012	11.2.0	-		12.0.0	Update to Rel-12 version (MCC)
2015-12	23.012	12.0.0	-		13.0.0	Update to Rel-13 version (MCC)
2017-03	23.012	13.0.0	-		14.0.0	Update to Rel-14 version (MCC)
2018-06	23.012	14.0.0	-	-	15.0.0	Update to Rel-15 version (MCC)